Einführung und Begriffe zur funktionalen Sicherheit von Maschinen und Anlagen

Nachschlagewerk · September 2010



Safety Integrated

Answers for industry.

SIEMENS

SIEMENS

Safety Integrated

Einführung und Begriffe zur funktionalen Sicherheit von Maschinen und Anlagen

Nachschlagewerk

www.siemens.de/safety-integrated

09/2010
E86060-T1813-A101-A3

Rechtliche Hinweise

Warnhinweiskonzept

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.

⚠GEFAHR
bedeutet, dass Tod oder schwere Körperverletzung eintreten **wird**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠WARNUNG
bedeutet, dass Tod oder schwere Körperverletzung eintreten **kann**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠VORSICHT
mit Warndreieck bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

VORSICHT
ohne Warndreieck bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

ACHTUNG
bedeutet, dass ein unerwünschtes Ergebnis oder Zustand eintreten kann, wenn der entsprechende Hinweis nicht beachtet wird.

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

Qualifiziertes Personal

Das zugehörige Gerät/System darf nur in Verbindung mit dieser Dokumentation eingerichtet und betrieben werden. Inbetriebsetzung und Betrieb eines Gerätes/Systems durfen nur von **qualifiziertem Personal** vorgenommen werden. Qualifiziertes Personal im Sinne der sicherheitstechnischen Hinweise dieser Dokumentation sind Personen, die die Berechtigung haben, Geräte, Systeme und Stromkreise gemäß den Standards der Sicherheitstechnik in Betrieb zu nehmen, zu erden und zu kennzeichnen.

Bestimmungsgemäßer Gebrauch von Siemens-Produkten

Beachten Sie Folgendes:

⚠WARNUNG
Das Gerät darf nur für die in der zugehörigen technischen Dokumentation vorgesehenen Einsatzfälle und nur in Verbindung mit von Siemens empfohlenen bzw. zugelassenen Fremdgeräten und –komponenten verwendet werden. Der einwandfreie und sichere Betrieb des Produkts setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung und Montage sowie sorgfälltige Bedienung und Instandhaltung voraus.

Marken

Alle mit dem Schutzrechtsvermerk ® gekennzeichneten Bezeichnungen sind eingetragene Marken der Siemens AG. Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Siemens AG
Industry Sector
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

Dokumentbestellnummer: E86060-T1813-A101-A3
℗ 09/2010

Inhaltsverzeichnis

Einleitung 1

1.1 Wichtige Hinweise

Die Informationen sind unverbindlich und erheben keinen Anspruch auf Vollständigkeit hinsichtlich Konfiguration und Ausstattung sowie jeglicher Eventualitäten. Die Informationen stellen keine kundenspezifische Lösungen dar, sondern sollen lediglich Hilfestellung bieten bei typischen Aufgabenstellungen. Sie sind für den sachgemäßen Betrieb der beschriebenen Produkte selbst verantwortlich. Diese Informationen entheben Sie nicht der Verpflichtung zu sicherem Umgang bei Anwendung, Installation, Betrieb und Wartung. Durch Nutzung dieser Informationen erkennen Sie an, dass Siemens über die oben beschriebene Haftungsregelung hinaus nicht für etwaige Schäden haftbar gemacht werden kann. Wir behalten uns das Recht vor, Änderungen an diesen Informationen jederzeit ohne Ankündigung durchzuführen. Bei Abweichungen zwischen den Vorschlägen in diesen Informationen und anderen Siemens Publikationen, wie z. B. Katalogen, hat der Inhalt der anderen Dokumentation Vorrang.

Erstell-Datum: 09/2010

1.2 Allgemeine Erläuterungen zu den Normen

pr	project, zeigt den Entwurfsstatus einer Norm
EN	Europäische Norm (gilt für alle europäischen Länder)
DIN EN	Deutsches Institut für Normung, Übersetzung der entsprechenden EN in die Landessprache Deutsch, gilt somit auch für alle europäischen Länder
ISO	International Organisation for Standardization, vorwiegend für Normen von elektromechanischen Systemen verantwortlich
IEC	International Engineering Consortium, Elektrische/Elektronische Systeme, vorwiegend für Normen von elektronischen Systemen verantwortlich (aber auch z. B. für Schütze)
DIN VDE	nationale Fassung einer IEC
AK (WG)	Arbeitskreis in Deutschland (Working Group)

Beispiel:

prEN ISO 13849-1

Dies ist ein Normentwurf prEN ISO 13849-1, den die ISO vorschlägt und in den nationalen Gremien berät. Nach Verabschiedung wird er zu der Norm EN ISO 13849-1.

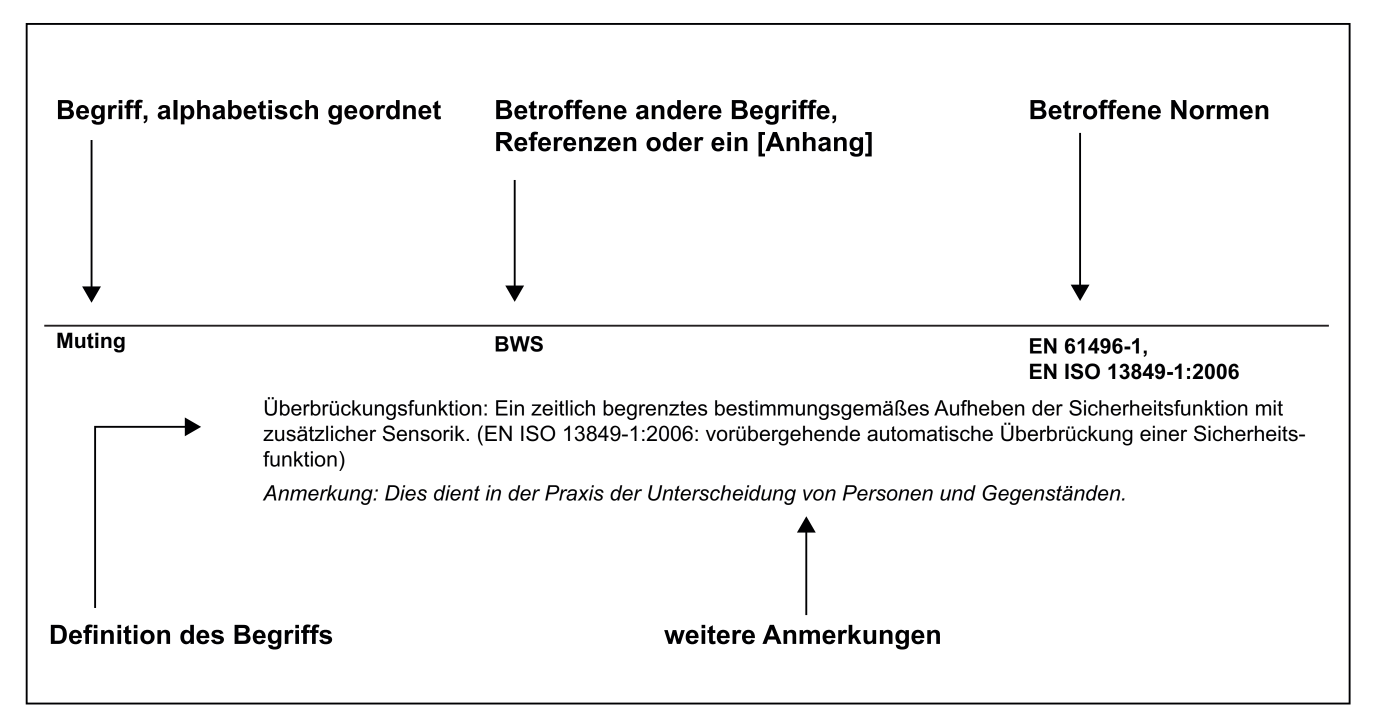
Mit ISO oder IEC wird die internationale Fassung einer Norm beschrieben. Wenn diese Norm in Europa unter der Maschinenrichtlinie gilt, dann wird diese als EN ISO bzw. EN bezeichnet.

Beispiel:

international	europäisch
ISO 13849-1	EN ISO 13849-1
IEC 62061	EN 62061

1.3 Erläuterungen zum Gebrauch der Broschüre

Im dritten Teil sind die Seiten mit Begriffserklärungen alphabetisch aufgebaut:



Im zweiten Teil sind noch folgende Anhänge beigefügt:

- Anhang 1: Wichtige Typ A, B und C-Normen
- Anhang 2: Weitere wichtige Dokumente
- Anhang 3: Risikobeurteilung nach EN ISO 12100, EN ISO 14121
- Anhang 4: Performance Level Bestimmung
- Anhang 5: SIL Zuordnung
- Anhang 6: Antriebssteuerungen mit integrierten Sicherheitsfunktionen
- Anhang 7: Bewertung von Sicherheitsfunktionen mit dem Safety Evaluation Tool
- Anhang 8: Englisch-Deutsch Wörterbuch

Vorschriften und Normen 2

2.1 Allgemeines

Zielsetzung der Sicherheitstechnik

Zielsetzung der Sicherheitstechnik soll es sein, die Gefährdung von Menschen und Umwelt durch technische Einrichtungen so gering wie möglich zu halten, ohne dadurch die industrielle Produktion, den Einsatz von Maschinen oder die Herstellung von chemischen Produkten mehr als unbedingt notwendig einzuschränken. Durch international abgestimmte Regelwerke soll der Schutz von Mensch und Umwelt allen Ländern in gleichem Maße zuteil werden und gleichzeitig sollen Wettbewerbsverzerrungen wegen unterschiedlicher Sicherheitsanforderungen im internationalen Handel vermieden werden.

In den verschiedenen Regionen und Ländern der Welt gibt es unterschiedliche Konzepte und Anforderungen zur Gewährleistung von Sicherheit. Die rechtlichen Konzepte und die Anforderungen wie und wann nachzuweisen ist, ob ausreichende Sicherheit besteht, sind ebenso unterschiedlich, wie die Zuordnung der Verantwortlichkeiten. So bestehen z. B. in der EU Anforderungen sowohl an den Hersteller einer Einrichtung als auch an den Betreiber, die durch europäische Richtlinien, Gesetze und Normen geregelt sind. In den USA bestehen dagegen regional und sogar lokal unterschiedliche Anforderungen.

Einheitlich in des gesamten USA ist jedoch der Grundsatz, dass ein Arbeitgeber Sicherheit am Arbeitsplatz gewährleisten muss. Im Falle eines Schadens kann, aufgrund der Produkthaftung, der Hersteller für den Schaden, der mit seinem Produkt in Verbindung gebracht werden kann, haftbar gemacht werden. In anderen Ländern oder Regionen gelten wiederum andere Prinzipien.

Wichtig für Hersteller von Maschinen und Errichter von Anlagen ist, dass immer die Gesetze und Regeln des Ortes gelten, an dem die Maschine oder Anlage betrieben wird. Beispielsweise muss die Steuerung einer Maschine, die in den USA betrieben werden soll, den dortigen Anforderungen genügen, auch wenn der Maschinenhersteller aus der EU stammt. Auch wenn die technischen Konzepte, mit denen Sicherheit erreicht wird, technischen Gesetzmäßigkeiten unterliegen, ist es trotzdem wichtig zu beachten, ob gesetzliche Regelungen mit bestimmten Vorgaben oder Restriktionen bestehen.

Sicherheitstechnik und funktionale Sicherheit

Die Sicherheit ist aus Sicht des zu schützenden Gutes unteilbar. Da die Ursachen von Gefährdungen und damit auch die technischen Maßnahmen zu ihrer Vermeidung aber sehr unterschiedlich sein können, unterscheidet man verschiedene Arten der Sicherheit, z. B. durch Angabe der jeweiligen Ursache möglicher Gefährdungen. So spricht man von "elektrischer Sicherheit", wenn der Schutz vor den Gefährdungen durch die Elektrizität zum Ausdruck gebracht werden soll, oder von "funktionaler Sicherheit", wenn die Sicherheit von der korrekten Funktion abhängt.

Diese Unterscheidung hat sich in der neueren Normung in der Art niedergeschlagen, dass es spezielle Normen gibt, die sich mit der funktionalen Sicherheit befassen. Im Bereich der Maschinensicherheit behandeln EN ISO 13849 (hervorgegangen aus EN 954) und IEC 62061 speziell die Anforderungen an sicherheitsrelevante Steuerungen und konzentrieren sich damit auf die funktionale Sicherheit. Das IEC behandelt in der Basis Sicherheitsnorm IEC 61508 (auch EN 61508 und DIN EN 61508 / VDE 0803) funktionale Sicherheit elektrischer, elektronischer und programmierbarer elektronischer Systeme unabhängig von einem speziellen Anwendungsgebiet.

Um funktionale Sicherheit einer Maschine oder Anlage zu erreichen, ist es notwendig, dass die sicherheitsrelevanten Teile der Schutz- und Steuereinrichtungen korrekt funktionieren und sich im Fehlerfall so verhalten, dass die Anlage in einem sicheren Zustand bleibt oder in einen sicheren Zustand gebracht wird.

Dazu ist die Verwendung besonders qualifizierter Technik notwendig, die den in den betreffenden Normen beschriebenen Anforderungen genügt. Die Anforderungen zur Erzielung funktionaler Sicherheit basieren auf den grundlegenden Zielen:

- Vermeidung systematischer Fehler
- Beherrschung systematischer Fehler
- Beherrschung zufälliger Fehler oder Ausfälle

Das Maß für die erreichte funktionale Sicherheit ist die Wahrscheinlichkeit gefährlicher Ausfälle, die Fehlertoleranz und die Qualität, durch die die Freiheit von systematischen Fehlern gewährleistet werden soll. Es wird in den Normen durch unterschiedliche Begriffe ausgedrückt. In IEC 61508: "Safety Integrity Level" (SIL), in EN 954: "Kategorien" und EN ISO 13849-1 "Performance Level" (PL).

Normen sorgen für Sicherheit

Aus der Verantwortung, die Hersteller und Betreiber technischer Einrichtungen und Produkte für die Sicherheit haben, resultiert die Forderung, Anlagen, Maschinen und andere technische Einrichtungen so sicher zu machen, wie es nach dem Stand der Technik möglich ist. Dazu wird von den Wirtschaftspartnern der Stand der Technik bezüglich aller Aspekte, die für die Sicherheit von Bedeutung sind, in Normen beschrieben. Durch Einhaltung der jeweils relevanten Normen kann dann sichergestellt werden, dass der Stand der Technik erreicht ist und damit der Errichter einer Anlage oder Hersteller einer Maschine oder eines Gerätes seine Sorgfaltspflicht erfüllt hat.

Hinweis

Die in diesem Nachschlagewerk aufgeführten Normen, Richtlinien und Gesetze sind eine Auswahl, um wesentliche Ziele und Prinzipien zu vermitteln. Die Liste erhebt keinen Anspruch auf Vollständigkeit.

2.2 Vorschriften und Normen in der Europäischen Union (EU)

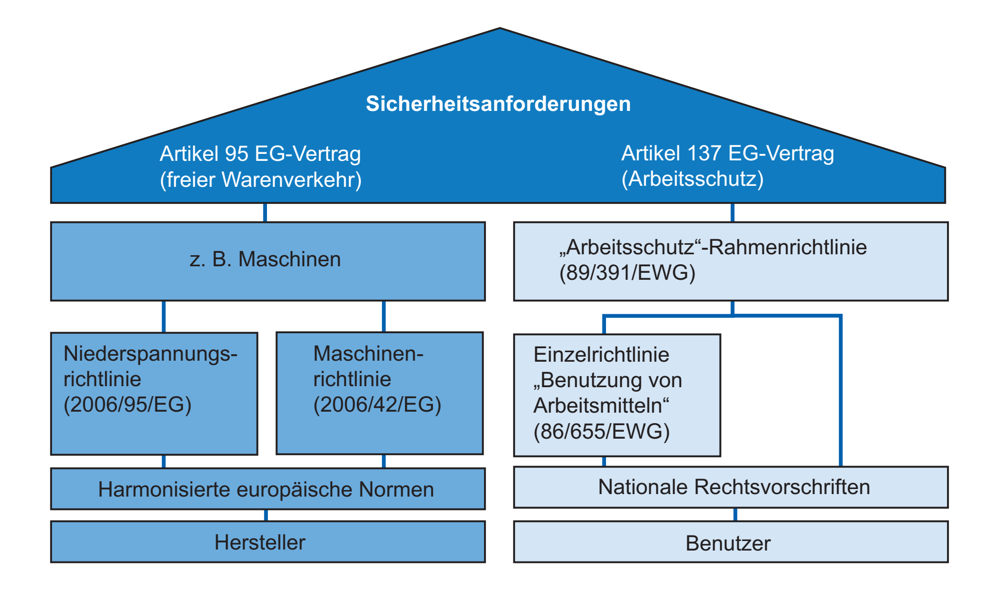


Bild 2-1 Normen und Vorschriften in Europa

2.2.1 Grundprinzipien der gesetzlichen Anforderungen in Europa

Die EFTA-Staaten haben sich dem Konzept der EU angeschlossen.

Die Gesetzgeber fordern, "durch vorbeugende Maßnahmen die Qualität der Umwelt und die Gesundheit des Menschen zu schützen" (Richtlinie 96/82/EG des Rates "Seveso II").

Sie fordern weiter "Sicherheit und Gesundheitsschutz der Beschäftigten bei der Arbeit" (Maschinenrichtlinie, Arbeitsschutzgesetze, ...). Die Erreichung dieser und ähnlicher Ziele wird in (EU-) Richtlinien vom Gesetzgeber für verschiedene Gebiete gefordert ("geregelter Bereich"). Zur Erreichung dieser Ziele stellt der Gesetzgeber Anforderungen an die Betreiber von Anlagen und die Hersteller von Geräten und Maschinen und hat gleichzeitig die Verantwortung für mögliche Schäden zugeordnet.

Die EU-Richtlinien

- legen Anforderungen an Anlagen und deren Betreiber zum Schutz der Gesundheit der Menschen und der Qualität der Umwelt fest;
- enthalten Bestimmungen über die Sicherheit am Arbeitsplatz (Mindestanforderungen);
- legen Produktanforderungen (z. B. für Maschinen) zum Schutz der Sicherheit und Gesundheit der Verbraucher fest;
- unterscheiden Anforderungen an die Realisierung von Produkten zur Gewährleistung des freien Warenverkehrs und Anforderungen an die Benutzung von Produkten.

Die EU-Richtlinen, die sich auf die Realisierung von Produkten beziehen, basieren auf Artikel 95 des EU-Vertrages, der den freien Warenverkehr regelt. Ihnen liegt ein neues, globales Konzept ("new approach", "global approach") zugrunde:

- EU-Richtlinien enthalten nur allgemeine Sicherheitsziele und legen grundlegende Sicherheitsanforderungen fest.
- Technische Details können von Normungsgremien, die ein entsprechendes Mandat der EU-Kommission haben (CEN, CENELEC), in Normen festgelegt werden. Diese Normen werden unter einer bestimmten Richtlinie harmonisiert und im Amtsblatt der EU gelistet. Bei Erfüllung der harmonisierten Normen gilt die Vermutung, dass die betreffenden Sicherheitsanforderungen der Richtlinien erfüllt sind. (Näheres siehe "Maschinensicherheit in Europa").
- Die Einhaltung bestimmter Normen ist nicht vom Gesetzgeber vorgeschrieben. Aber bei Einhaltung bestimmter Normen "darf vermutet werden", dass die betreffenden Sicherheitsziele der EU-Richtlinien erfüllt sind.
- EU-Richtlinien verlangen von den Mitgliedsländern die gegenseitige Anerkennung nationaler Vorschriften.

Neben den gerätetypspezifischen Richtlinien wie z. B. Niederspannungsrichtlinie oder Maschinenrichtlinie, auf die im Folgenden näher eingegangen wird, gibt es auch eine allgemeine "Produktsicherheitsrichtlinie", in der allgemeine Fragen zur Produktsicherheit geregelt sind. Sie ist in Deutschland im Geräte- und Produktsicherheitsgesetz (GPSG) umgesetzt.

Die EU-Richtlinien sind nebeneinander gleichwertig, d.h., wenn mehrere Richtlinien für eine bestimmte Einrichtung zutreffen, gelten die Anforderungen aller relevanten Richtlinien (z. B. für eine Maschine mit elektrischer Ausrüstung gilt die Maschinenrichtlinie und die Niederspannungsrichtlinie).

Für Einrichtungen, die nicht zum Geltungsbereich der EU-Richtlinien gehören, gibt es Verordnungen. Sie enthalten Bestimmungen und Kriterien für freiwillige Prüfungen und Zertifizierungen.

Die EU-Richtlinien des New Approach mit den zugehörigen Listen der harmonisierten Normen findet man im Internet unter: (http://www.newapproach.org/).

2.2.2 Arbeitsschutz in der EU

Die Anforderungen zur Sicherheit am Arbeitsplatz basieren auf Artikel 137 (früher 118a) des EU-Vertrages. Die Rahmenrichtlinie "Sicherheits- und Gesundheitsschutz der Arbeitnehmer" (89/391/EWG) legt Mindestanforderungen für Sicherheit am Arbeitsplatz fest. Die tatsächlichen Anforderungen unterliegen der nationalen Gesetzgebung und können die Anforderungen der Rahmenrichtlinie übersteigen. Diese Anforderungen betreffen das Betreiben von Produkten (z. B. Maschinen, Chemieanlagen), nicht deren Realisierung.

In Deutschland sind die Anforderungen in der Betriebssicherheitsverordnung (BetrSichV) zusammengefasst. Nähere Informationen dazu finden sich auf den Internetseiten der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BauA) (http://www.baua.de/baua/index.htm).

2.2.3 Maschinensicherheit in Europa

Maschinenrichtlinie (2006/42/EG)

Mit der Einführung des einheitlichen europäischen Binnenmarktes wurde beschlossen, dass die nationalen Normen und Vorschriften aller EG-Mitgliedsstaaten, die die technische Realisierung von Maschinen betreffen, harmonisiert werden. Dies hatte zur Folge, dass die Maschinenrichtlinie als eine Binnenmarktrichtlinie von den einzelnen Mitgliedsstaaten inhaltlich in nationales Recht umgesetzt werden musste. In Deutschland wurde der Inhalt der Maschinenrichtlinie als 9. Verordnung zum Gerätesicherheitsgesetz umgesetzt. Dies geschah bei der Maschinenrichtlinie vor dem Hintergrund einheitlicher Schutzziele mit dem Zweck, technische Handelshemmnisse abzubauen. Der Anwendungsbereich der Maschinenrichtlinie ist entsprechend ihrer Definition "Maschine ist eine Gesamtheit von miteinander verbundenen Teilen oder Vorrichtungen, von denen mindestens eines beweglich ist" sehr weit gefasst.

Als "Maschine" wird auch eine Gesamtheit von Maschinen bezeichnet, die, damit sie zusammenwirken, so angeordnet sind und betätigt werden, dass sie als Gesamtheit funktionieren.

Der Anwendungsbereich der Maschinenrichtlinie erstreckt sich somit von einer "unvollständigen" Maschine bis hin zu einer Anlage.

Seit dem 29. Dezember 2009 gelten die Anforderungen der neuen Maschinenrichtlinie 2006/42/EG für die funktionale Sicherheit.

Die Neuerungen betreffen die Risikobeurteilung, Anforderungen an die Dokumentation und geeignete Sicherheitssysteme, die Konformitätsbewertung sowie Maschinenbauer außerhalb der Europäischen Union. Die Risikobeurteilung einer Maschine muss durch kompetentes Fachpersonal vorgenommen werden. Die Durchführung der Risikobeurteilung muss in der technischen Dokumentation der Maschine beschrieben und in der Betriebsanleitung erwähnt werden.

Für die CE Konformitätsbewertung wurden neue Verfahren definiert. Diese gelten für Maschinen, die im Anhang IV der Maschinenrichtlinie gelistet wurden sowie für "unvollständige Maschinen". Maschinenhersteller, die Maschinen von außerhalb in die EU importieren möchten, müssen die technische Dokumentation ihrer Maschine in der EU, z. B. durch Bevollmächtigte, erstellen lassen. Dies vereinfacht das CE-Konformitätsverfahren bei Behörden und sorgt beim Anwender für mehr Sicherheit beim Kauf und Betrieb der Maschine.

Die Erfüllung der grundlegenden Sicherheits- und Gesundheitsanforderungen in Anhang I der Richtlinie ist für die Sicherheit von Maschinen zwingend notwendig. Der Hersteller muss folgende Grundsätze für die Integration der Sicherheit beachten:

1. "Durch die Bauart der Maschine muss gewährleistet sein, dass Betrieb, Rüsten und Wartung bei bestimmungsgemäßer Verwendung ohne Gefährdung von Personen erfolgen." "Die Maßnahmen müssen ... Unfallrisiken ... ausschließen..."
2. "Bei der Wahl der angemessenen Lösungen muss der Hersteller folgende Grundsätze anwenden, und zwar in der angegebenen Reihenfolge:
   - Beseitigung oder Minimierung der Gefahren (Integration des Sicherheitskonzepts in die Entwicklung und den Bau der Maschine)
   - Ergreifen von notwendigen Schutzmaßnahmen gegen nicht zu beseitigende Gefahren
   - Unterrichtung der Benutzer über die Restgefahren aufgrund der nicht vollständigen Wirksamkeit der getroffenen Sicherheitsmaßnahmen

Die Schutzziele müssen verantwortungsbewusst umgesetzt werden, um die Forderung nach Konformität mit der Richtlinie zu erfüllen.

Der Hersteller einer Maschine muss den Nachweis über die Übereinstimmung mit den grundlegenden Anforderungen erbringen. Dieser Nachweis wird durch die Anwendung harmonisierter Normen (wie z. B. die EN ISO 13849-1 oder EN 62061) erleichtert.

Normen

Um Produkte in den Verkehr bringen oder betreiben zu dürfen, müssen sie den grundlegenden Sicherheitsanforderungen der EU-Richtlinien entsprechen. Zur Erfüllung dieser Sicherheitsanforderungen können Normen sehr hilfreich sein. Dabei ist in der EU zu unterscheiden zwischen Normen, die unter einer EU-Richtlinie harmonisiert sind und Normen, die zwar ratifiziert, aber nicht unter einer bestimmten Richtlinie harmonisiert sind, sowie sonstigen technischen Regeln, in den Richtlinien auch "nationale Normen" genannt.

Ratifizierte Normen beschreiben den anerkannten Stand der Technik. D. h. der Hersteller kann durch ihre Anwendung nachweisen, dass er den anerkannten Stand der Technik erfüllt hat.

Grundsätzlich müssen alle Normen, die als Europanormen ratifiziert sind, in die nationalen Normenwerke der Mitgliedsstaaten unverändert übernommen werden, unabhängig davon, ob sie unter einer Richtlinie harmonisiert sind oder nicht. Bestehende nationale Normen zum gleichen Thema müssen dann zurückgezogen werden. So soll im Laufe der Zeit in Europa ein einheitliches (widerspruchsfreies) Normenwerk geschaffen werden.

Hinweis

Eine wichtige nicht unter einer EU-Richtlinie harmonisierte Norm ist IEC 61508 "Functional safety of electrical/electronic/programmable electronic safety-related systems". Sie ist als EN 61508 ratifiziert. Dort, wo EN 61508 in einer harmonisierten Norm referenziert wird, ist sie eine "mitgeltende" Norm zu der betreffenden harmonisierten Norm.

Harmonisierte Europanormen

Sie werden von den beiden Normungsorganisationen CEN (Comité Européen de Normalisation) und CENELEC (Comité Européen de Normalisation Electrotechnique) im Auftrag der EU-Kommission erarbeitet, um die Anforderungen der EU-Richtlinien für ein bestimmtes Produkt zu präzisieren. Diese Normen (EN-Normen) werden im Amtsblatt der europäischen Gemeinschaften veröffentlicht und sind danach ohne Änderungen in nationale Normen zu übernehmen.

Sie dienen zur Erfüllung der grundlegenden Sicherheits- und Gesundheitsanforderungen und der im Anhang I der Maschinenrichtlinie genannten Schutzziele.

Der Ansprechpartner für CEN/CENELEC in Deutschland ist das DIN und die DKE.

Durch Einhaltung der harmonisierten Normen ergibt sich eine "automatische Vermutungswirkung" der Erfüllung der Richtlinie, d. h., der Hersteller darf darauf vertrauen, dass er die Sicherheitsaspekte der Richtlinie erfüllt hat, soweit sie in der jeweiligen Norm behandelt sind. Allerdings ist nicht jede Europanorm in diesem Sinne harmonisiert. Entscheidend ist die Listung im europäischen Amtsblatt. Diese Listen sind stets aktuell im Internet (http://www.newapproach.org/) abrufbar.

Das europäische Normenwerk für Sicherheit von Maschinen ist hierarchisch aufgebaut, es gliedert sich in

- A-Normen,
  auch Grundnormen genannt.
- B-Normen,
  auch Gruppennormen genannt.
- C-Normen,
  auch Produktnormen genannt.

Den Aufbau zeigt die folgende Darstellung.

Sicherheits-grundnormen	Typ-A-Normen Grundlegende Festlegungen für alle Maschinen	EN ISO 12100 Sicherheit von Maschinen - Grundbegriffe, allgemeine Gestaltungsleitsätze EN ISO 14121 Sicherheit von Maschinen - Leitsätze zur Risikobeurteilung				
Sicherheits-gruppennormen	Typ-B1-Normen Übergeordnete Sicherheitsaspekte	Mindestab-stände zur Vermeidung des Quetschens von Körperteilen EN 349	Sicherheitsrele-vante Teile von Steuerungen EN 62061 EN ISO 13849-1[1]	Sicherheits-abstände gegen das Erreichen von Gefahren-stellen mit den oberen Gliedmaßen EN 294	Elektrische Ausrüstung von Maschinen EN 60204-1	Sicherheit von Maschinen-Verriege-lungseinrich-tungen mit und ohne Zuhaltung EN 1088
	Typ-B2-Normen Anforderungen für Sicherheitsgeräte (Bezug auf spezielle Schutzeinrichtungen)	Zweihand-schaltung EN 574	NOT-HALT-Einrichtung, funktionelle Aspekte - Gestaltungsleitsätze - EN ISO 13850		Lichtschranken, Lichtvorhänge EN 61496-1	
Fachnormen	Typ-C-Normen Fachnormen Spezifische Anforderungen an bestimmte Maschinen	Aufzüge EN 81-3	Spritzgieß-maschinen EN 201	Pressen & Scheren EN 692 EN 693	Numerisch gesteuerte Drehmaschinen EN 12415, EN 12418	

[1] Übergangsfrist zur Verwendung der EN 954-1 endet am 31.12.2011.

Bild 2-2 Das europäische Normenwerk für Sicherheit von Maschinen

Zu Typ-A-Normen/Grundnormen

A-Normen enthalten grundlegende Begriffe und Festlegungen für alle Maschinen. Dazu zählt die EN ISO 12100 "Sicherheit von Maschinen, Grundbegriffe, allgemeine Gestaltungsleitsätze."

A-Normen richten sich primär an die Normensetzer von B- und C-Normen. Die dort niedergelegten Verfahren zur Risikominimierung können jedoch auch für den Hersteller hilfreich sein, wenn keine C-Normen vorliegen.

Zu Typ-B-Normen/Gruppennormen

Das sind alle Normen mit sicherheitstechnischen Aussagen, die mehrere Arten von Maschinen betreffen können.

Auch die B-Normen richten sich primär an die Normensetzer für C-Normen. Sie können jedoch auch für Hersteller bei Konstruktion und Bau einer Maschine hilfreich sein, wenn keine C-Normen vorliegen.

Es wurde bei den B-Normen eine weitere Unterteilung vorgenommen, und zwar in:

Typ-B1-Normen für übergeordnete Sicherheitsaspekte, z. B. ergonomische Grundsätze, Sicherheitsabstände gegen das Erreichen von Gefahrquellen, Mindestabstände zur Vermeidung des Quetschens von Körperteilen.

Typ-B2-Normen für Sicherheitseinrichtungen sind bestimmt für verschiedene Maschinenarten, z. B. Not-Halt-Einrichtungen, Zweihandschaltungen, Verriegelungen, berührungslos wirkende Schutzeinrichtungen, sicherheitsbezogene Teile von Steuerungen.

Zu Typ-C-Normen/Produktnormen

Hierbei handelt es sich um maschinenspezifische Normen z. B. für Werkzeugmaschinen, Holzbearbeitungsmaschinen, Aufzüge, Verpackungsmaschinen, Druckmaschinen u. ä.

Das europäische Normenwerk ist so aufgebaut, dass, um Wiederholungen allgemeiner Aussagen zu vermeiden, die in Typ-A- oder Typ-B-Normen bereits enthalten sind, in den Typ-C-Normen soweit wie möglich darauf verwiesen wird.

Produktnormen enthalten maschinenspezifische Anforderungen. Die Anforderungen können unter Umständen von den Grund- und Gruppennormen abweichen. Für den Maschinenbauer hat die Typ-C-Norm/Produktnorm die absolut höhere Priorität. Er darf davon ausgehen, dass er damit die grundlegenden Anforderungen des Anhangs I der Maschinenrichtlinien einhält (automatische Vermutungswirkung). Liegt für eine Maschine keine Produktnorm vor, so können Typ-B-Normen als Hilfen für den Bau einer Maschine herangezogen werden.

Um ein Mittel der Übereinstimmung mit den grundlegenden Anforderungen der Richtlinie bereitzustellen, werden für Maschinen oder Maschinengruppen nahezu aller Bereiche mit dem Mandat der EU-Kommission harmonisierte Normen in technischen Komitees des CEN und CENELEC erarbeitet. An der Erarbeitung sind in erster Linie Vertreter der Hersteller der betreffenden Maschinen, der Aufsichtsbehörden wie Berufsgenossenschaften sowie der Betreiber beteiligt. Eine vollständige Liste aller gelisteten Normen sowie der mandatierten Normungsvorhaben finden Sie im Internet unter: (http://www.newapproach.org/).

Empfehlung: Wegen der rasch fortschreitenden technischen Entwicklung und den damit verbundenen Änderungen von Maschinenkonzepten sollte bei Anwendung besonders von C-Normen deren Aktualität geprüft werden. Gegebenenfalls ist zu beachten, dass die Anwendung der Norm nicht zwingend ist, sondern das Sicherheitsziel erreicht werden muss.

Nationale Normen

Fehlen harmonisierte Europanormen oder können sie aus bestimmten Gründen nicht angewendet werden, so kann sich ein Hersteller der "nationalen Normen" bedienen. Unter diesen Begriff der Maschinenrichtlinie fallen alle anderen technischen Regeln, z. B. auch die Unfallverhütungsvorschriften und nicht im europäischen Amtsblatt gelistete Normen (auch IEC oder ISO Normen, die als EN ratifiziert wurden). Durch Anwendung ratifizierter Normen kann der Hersteller nachweisen, dass der anerkannte Stand der Technik erfüllt wurde. Die Anwendung dieser Normen führt nicht zwangsläufig zu einer Vermutungswirkung, wie mit einer harmonisierten Norm.

Risikobeurteilung

Maschinen und Anlagen beinhalten aufgrund ihres Aufbaus und ihrer Funktionalität Risiken. Deshalb verlangt die Maschinenrichtlinie für jede Maschine eine Risikobeurteilung und gegebenenfalls eine Risikominderung, bis das Restrisiko kleiner als das tolerierbare Risiko ist.

Für die Verfahren der Bewertung dieser Risiken sind folgende Normen anzuwenden:

- EN ISO 12100 "Sicherheit von Maschinen – Grundbegriffe, allgemeine Gestaltungsleitsätze"
- EN ISO 14121 "Sicherheit von Maschinen, Leitsätze zur Risikobeurteilung"

Schwerpunktmäßig beschreibt EN ISO 12100 die zu betrachtenden Risiken und Gestaltungsleitsätze zur Risikominderung, EN ISO 14121 den iterativen Prozess mit Risikobeurteilung und Risikominderung zum Erreichen der Sicherheit.

Prozess der Risikobeurteilung

Die Risikobeurteilung ist eine Folge von Schritten, welche die systematische Untersuchung von Gefährdungen erlauben, die von Maschinen ausgehen. Wo notwendig, folgt einer Risikobeurteilung eine Risikoreduzierung. Bei Wiederholung dieses Vorgangs ergibt sich der iterative Prozess (siehe Bild 2/4), mit dessen Hilfe Gefährdungen so weit wie möglich beseitigt werden können und entsprechende Schutzmaßnahmen getroffen werden können.

Die Risikobeurteilung umfasst die

- Risikoanalyse
  - Bestimmung der Grenzen der Maschine (EN ISO 12100, EN ISO 14121 Abs. 5)
  - Identifizierung der Gefährdungen (EN ISO 12100, EN ISO 14121 Abs. 6)
  - Verfahren zur Risikoeinschätzung (EN ISO 14121 Abs. 7)
- Risikobewertung (EN ISO 14121 Abs. 8)

Gemäß dem iterativen Prozess zum Erreichen der Sicherheit erfolgt nach der Risikoeinschätzung eine Risikobewertung. Dabei muss entschieden werden, ob eine Risikominderung notwendig ist. Falls das Risiko weiter vermindert werden soll, sind geeignete Schutzmaßnahmen auszuwählen und anzuwenden. Die Risikobeurteilung ist dann zu wiederholen.

Als Hilfe zur Risikobewertung sind Risikoelemente definiert. Den Zusammenhang dieser Risikoelemente verdeutlicht folgendes Bild.

Die Risikoelemente (S, F und W) dienen als Eingangsgröße für beide Normen. Die Bewertung dieser Risikoelemente erfolgt auf unterschiedliche Art und Weise. Nach EN 62061 wird ein geforderter Sicherheitsintegritäts-Level (SIL) bestimmt, nach EN ISO 13849-1 ein Performance Level (PL).

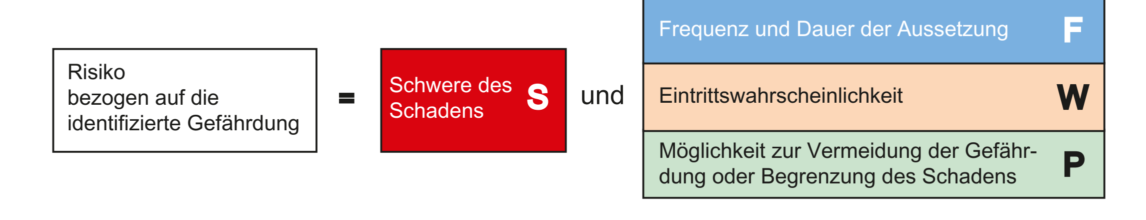


Bild 2-3 Risikoelemente

Ist die erforderliche Sicherheit noch nicht erreicht, sind Maßnahmen zur Risikominderung erforderlich.

Die Risikominderung muss durch geeignete Konzipierung und Realisierung der Maschine erfolgen, z. B. durch für Sicherheitsfunktionen geeignete Steuerung oder Schutzmaßnahmen.

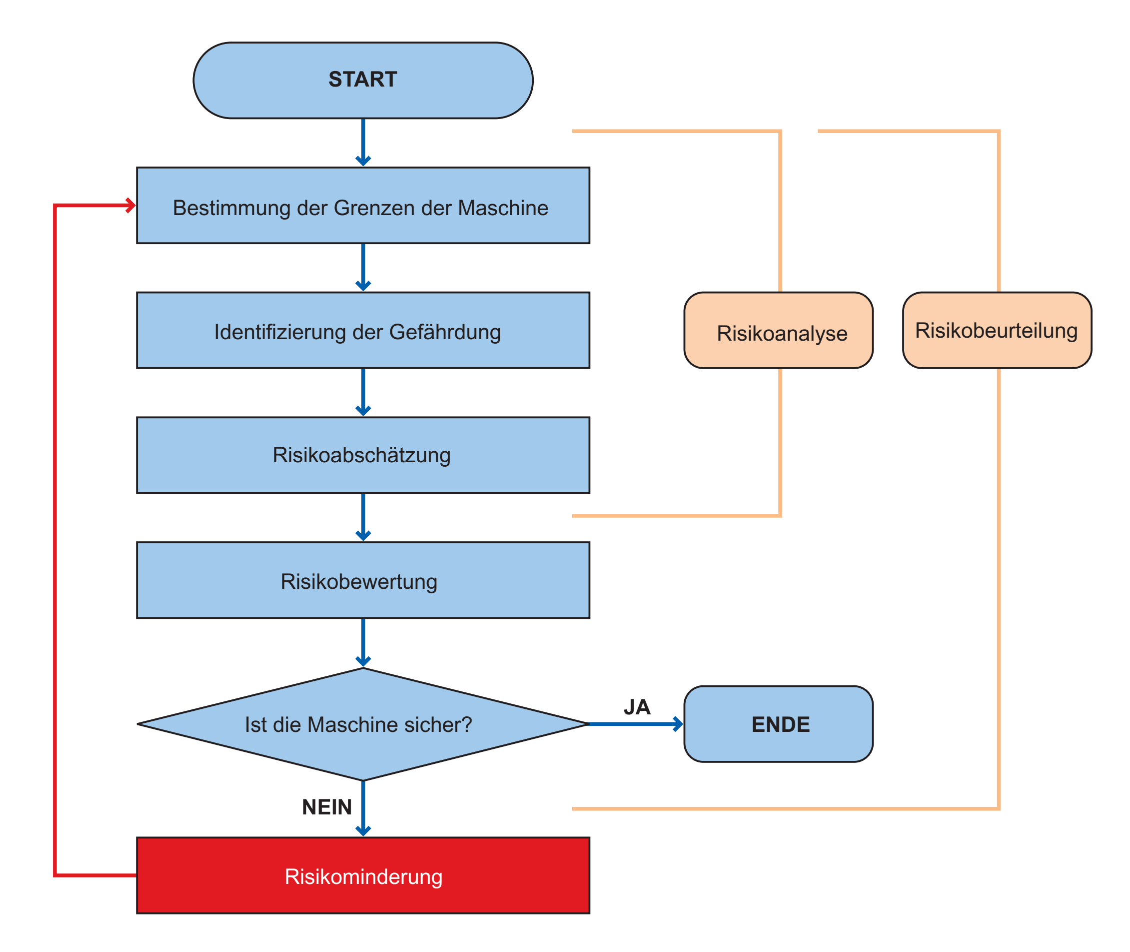


Bild 2-4 Interaktiver Prozess zum Erreichen der Sicherheit nach EN ISO 14121

Restrisiko (EN ISO 14121)

Sicherheit ist ein relativer Begriff unserer technisierten Welt. Sicherheit so zu realisieren, dass unter keinen Umständen etwas passieren kann, sozusagen die "Null-Risiko-Garantie", ist leider nicht durchführbar. Das verbleibende Restrisiko ist definiert als: Risiko, das nach Ausführung der Schutzmaßnahmen verbleibt. Hierbei sind unter Schutzmaßnahmen alle Maßnahmen zur Risikominderung zu verstehen.

2.2.4 Funktionale Sicherheit - elektrische Sicherheit

Risikominderung

Die Risikominderung einer Maschine kann, außer durch strukturelle Maßnahmen, auch durch sicherheitsrelevante Steuerungsfunktionen erfolgen. Für die Realisierung dieser Steuerungsfunktionen sind, abgestuft nach der Höhe des Risikos, besondere Anforderungen zu beachten, die in EN ISO 13849-1 und, für elektrische Steuerungen insbesondere mit programmierbarer Elektronik, in IEC 61508 beschrieben sind.

Die Anforderungen an sicherheitsrelevante Teile von Steuerungen sind nach der Höhe des Risikos bzw. der notwendigen Risikominderung abgestuft. Die bisher gültige EN 954-1 definiert dazu "Kategorien" und beschreibt in ihrem Anhang B ein Verfahren zur Auswahl der geeigneten Kategorie für die Gestaltung der sicherheitsbezogenen Teile einer Steuerung. Mit der Nachfolgenorm EN ISO 13849-1 wurde ein neuer Risikograf eingeführt, der anstelle der Kategorien zu hierarchisch abgestuften Performance Leveln (PL) führt (siehe Anhang 4.4.).

Die EN 62061 verwendet den "Safety Integrity Level" (SIL) zur Risikoeinstufung (siehe Anhang 4.5.). Das ist ein quantifiziertes Maß für die sicherheitsbezogene Leistungsfähigkeit einer Sicherheitsfunktion. Die Ermittlung des notwendigen SIL erfolgt ebenfalls nach dem Prinzip der Risikobewertung gemäß EN ISO 14121. Im Anhang A der Norm ist ein Verfahren zur Bestimmung des notwendigen Safety Integrity Level beschrieben.

Wichtig ist in jedem Fall, unabhängig davon welche Norm angewendet wird, dass alle Teile der Steuerung der Maschine, die an der Ausführung der sicherheitsrelevanten Funktionen beteiligt sind, diesen Anforderungen genügen.

Hinweis

Zur Steuerung einer Maschine gehören auch die Laststromkreise der Antriebe und Motoren.

Beim Entwurf und der Realisierung der Steuerung ist es notwendig zu überprüfen, ob die Anforderungen des ausgewählten PL bzw. SIL erfüllt sind.

In den Normen sind neuartige Aspekte zu beachten, damit

- zufällige Ausfälle der Hardware beherrscht,
- systematische Fehler in der Hardware und der Software vermieden und
- systematische Fehler in der Hardware und der Software beherrscht werden.

Validierung

Validierung bedeutet eine bewertende Überprüfung der angestrebten Sicherheitsfunktionalität. Ihr Zweck ist, die Festlegungen und das Niveau der Konformität der sicherheitsbezogenen Teile der Steuerung innerhalb der Gesamtfestlegung für Sicherheitsanforderungen an der Maschine zu bestätigen. Die Validierung muss weiterhin aufzeigen, dass jedes sicherheitsbezogene Teil die Anforderungen der relevanten Norm erfüllt.

Dabei sind die folgenden Aspekte beschrieben:

- Fehlerlisten
- Validierung der Sicherheitsfunktionen
- Validierung der geforderten und der erreichten Safety Performance (Kategorie, Safety Integrity Level oder Performance Level)
- Validierung der Umgebungsanforderungen
- Validierung der Instandhaltungsanforderungen

In einem Validierungsplan müssen die Anforderungen für die Durchführung der Validierung für die festgelegten Sicherheitsfunktionen beschrieben werden.

Safety Integrated

Die Maßnahmen, um eine komplexe Steuerung für Sicherheitsaufgaben ausreichend funktionssicher zu machen, sind sehr umfangreich und betreffen das Konzept sowie den gesamten Entwicklungs- und Herstellungsprozess. Solche Geräte werden deshalb speziell für Sicherheitsfunktionen konzipiert. Beispiele sind SIMATIC S7 300F / S7 400F/FH und SINUMERIK "Safety Integrated" sowie die Kommunikationssysteme PROFIsafe und ASI-safe, die PROFIBUS und AS-Interface zur Übertragung sicherheitsbezogener Daten verwenden.

Sicherheitsbezogene Funktionen

Die sicherheitsbezogenen Funktionen umfassen neben den klassischen Funktionen

- Stillsetzen
- Handlungen im Notfall
- Verhindern unbeabsichtigten Anlaufs

inzwischen auch komplexere Funktionen wie:

- Zustandsabhängige Verriegelungen
- Geschwindigkeitsbegrenzung
- Positionsbegrenzung
- Kontrolliertes Stillsetzen
- Kontrolliertes Halten u. ä.

Die klassischen Funktionen sind u.a. in EN 60204-1 definiert und wurden bisher im Allgemeinen durch einfache elektromechanische Bauteile realisiert. Sie können aber, ebenso wie komplexere Funktionen, auch durch programmierbare elektronische Systeme realisiert werden, wenn diese die relevanten Normen erfüllen. Komplexe Funktionen, die z. B. das Verhalten drehzahlveränderbarer Antriebe betreffen, werden in EN 61800-5-2 beschrieben.

Stillsetzen

Stopp-Kategorien der EN 60204-1

Zum Stillsetzen einer Maschine sind in EN 60204-1 (VDE 0113 Teil 1) drei Stopp-Kategorien definiert, die den Steuerablauf für das Stillsetzen unabhängig von einer Notfallsituation beschreiben.

Stopp-Kategorie 0	Ungesteuertes Stillsetzen durch sofortige Abschaltung der Energie zu den Maschinenantriebselementen.
Stopp-Kategorie 1	Gesteuertes Stillsetzen; Energiezufuhr wird erst dann unterbrochen, wenn Stillstand erreicht ist.
Stopp-Kategorie 2	Gesteuertes Stillsetzen, bei dem die Energiezufuhr im Stillstand erhalten bleibt. **Hinweis:** Durch das Abschalten wird nur die Zufuhr der Energie, die eine Bewegung verursachen kann, unterbrochen. Es wird nicht spannungsfrei geschaltet.

Handlung im Notfall

Eine Handlung im Notfall (EN 60204-1) kann wie folgt beschrieben werden:

- Stillsetzen im Notfall (Not-Halt)
- Ingangsetzen im Notfall (Not-Start)
- Ausschalten im Notfall (Not-Aus)
- Einschalten im Notfall (Not-Ein)

Diese Funktionen werden nach EN 60204-1 und EN ISO 13850 ausschließlich durch eine bewusste menschliche Handlung ausgelöst. Im Folgenden wird nur auf das "Ausschalten im Notfall" und auf das "Stillsetzen im Notfall" weiter eingegangen.

Hinweis

In Deutschland wird für das "Stillsetzen im Notfall" neben dem Begriff Not-Halt häufig auch der Begriff Not-Aus verwendet, auch wenn damit nur das Stillsetzen gemeint ist.

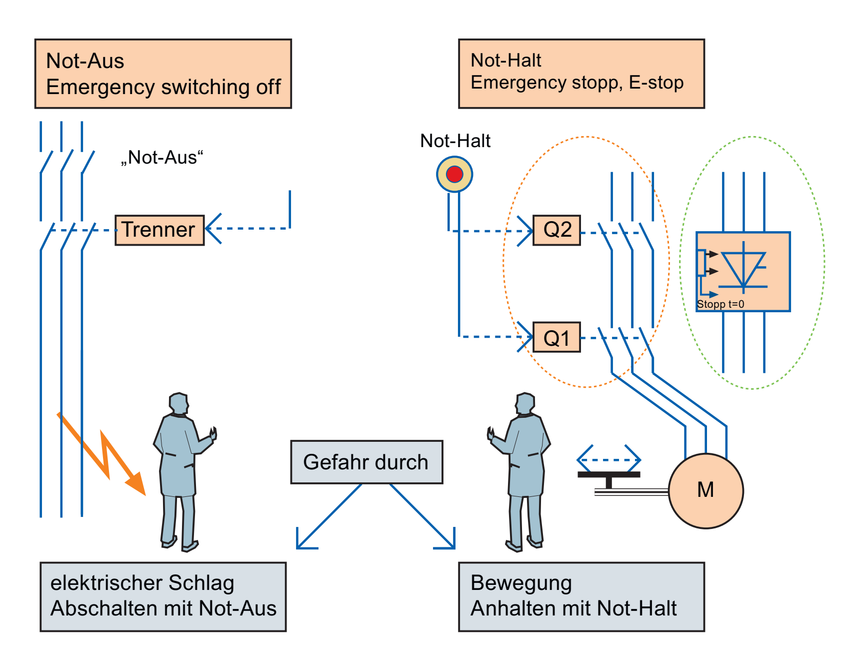


Bild 2-5 Unterscheidung Not-Aus und Not-Halt

Not-Aus

Eine Handlung im Notfall, die dazu bestimmt ist, die Versorgung mit elektrischer Energie zu einer ganzen oder zu einem Teil einer Installation abzuschalten, falls ein Risiko für elektrischen Schlag oder ein anderes Risiko elektrischen Ursprungs besteht (siehe auch EN 60204-1 Anhang D).

Funktionale Aspekte zum Ausschalten im Notfall sind in IEC 60364-4-46 (identisch mit HD 384-4-46 und VDE 0100 Teil 460) festgelegt.

Ein Ausschalten im Notfall ist vorzusehen, wo

- Schutz gegen direktes Berühren (z. B. mit Schleifleitungen, Schleifringkörpern, Schaltgeräten in elektrischen Betriebsräumen) nur durch Abstand oder Hindernisse erreicht wird.
- es die Möglichkeit anderer Gefährdungen oder Beschädigungen durch elektrische Energie gibt.

Not-Halt

Eine Handlung im Notfall, die dazu bestimmt ist, einen Prozess oder eine Bewegung anzuhalten, der (die) gefahrbringend wurde (aus EN 60204-1).

Zusätzlich zu den Anforderungen für Stopp gelten für das Stillsetzen im Notfall folgende Anforderungen:

- Es muss gegenüber allen anderen Funktionen und Betätigungen in allen Betriebsarten Vorrang haben;
- Die Energie zu den Maschinen-Antriebselementen, die einen gefahrbringenden Zustand bzw. gefahrbringende Zustände verursachen können, muss ohne Erzeugung anderer Gefährdungen so schnell wie möglich abgeschaltet werden (z. B. durch mechanische Anhaltevorrichtungen, die keine externe Versorgung erfordern, durch Gegenstrombremsen bei Stopp-Kategorie 1);
- Das Rücksetzen darf keinen Wiederanlauf einleiten.

Für die technische Realisierung des Not-Halt können, entsprechend der Anwendungsempfehlung im Vorwort von EN 60204-1, entweder die Anforderungen in EN 60204-1 oder in EN ISO 13849-1 und IEC 61508 angewendet werden. EN 60204-1 Ausgabe 4 fordert vorrangig die Realisierung durch elektromechanische Komponenten, da "einfache" (programmierbare) elektronische Systeme nicht sicher genug sind. Durch die richtige Anwendung von EN ISO 13849-1 und ggf. IEC 61508 werden elektronische und programmierbare elektronische Komponenten so funktionssicher, dass sie ebenfalls zur Realisierung des Not-Halt für alle Kategorien eingesetzt werden.

Geräte für Not-Aus und Not-Halt

Geräte für das Stillsetzen im Notfall müssen an jedem Bedienstand sowie an anderen Orten, wo die Einleitung eines Stillsetzens im Notfall erforderlich sein kann, vorhanden sein (Ausnahme: kabellose Bedienstationen).

Um die Schutzziele sowohl der EN 60204-1 als auch der EN ISO 13850 zu erfüllen, gelten für beide Funktionen folgende Anforderungen:

- Bei einem Schalten der Kontakte, auch bei einer nur kurzen Betätigung, muss das Befehlsgerät zwangsweise verrasten.
- Es darf nicht möglich sein, dass die Maschine von einem entfernten Hauptbedienstand wieder gestartet wird, ohne dass die Gefahr vorher beseitigt wurde. Die Notschalteinrichtung muss "vor Ort" durch eine bewusste Handlung wieder entriegelt werden.

Kabellose Bedienstationen müssen eine eigene und eindeutig erkennbare Möglichkeit haben, um die Stopp-Funktion der Maschine einzuleiten. Das Bedienteil, das diese Stopp-Funktion einleitet, darf nicht als Einrichtung zum Stillsetzen im Notfall markiert oder beschriftet sein.

Mensch – Maschine (Farbkennzeichnung für Bedienteile und Anzeigen)

Um das Zusammenwirken zwischen Mensch und Maschine zu erleichtern, werden in den Normen EN 60073 sowie DIN EN 60204-1 Vorgaben zur Kennzeichnung und Codierung gemacht.

Zu den Maschinenkomponenten, die im Schnittstellenbereich Mensch – Maschine eingesetzt werden, zählen in erster Linie Schalter, Taster und Leuchtmelder. Die durchgängige eindeutige Kennzeichnung dieser Bedienelemente erfolgt durch farbliche Kennzeichnung, die einer konkreten Bedeutung zugeordnet sind. Dadurch ist gewährleistet, dass die Sicherheit des Bedienpersonals erhöht und die Bedienung und Wartung der Betriebsmittel/Anlagen erleichtert werden.

Die Farben für Drucktaster, die Bedeutung der Farben sowie Erklärungen und Anwendungsbeispiele werden in den folgenden Tabellen angegeben.

In Tabelle "Farben für Leuchtmelder und ihre Bedeutung nach EN 60204-1 (VDE 0113 Teil 1)" werden die Farben für Leuchtmelder, ihre Bedeutung in Bezug auf den Zustand der Maschine sowie Handhabung und Anwendungsbeispiele aufgeführt.

Bei Leuchtdrucktastern gelten ebenfalls die beiden folgenden Tabellen.

Farbe	Bedeutung	Erklärung	Anwendungsbeispiele
ROT	Notfall	Bei gefährlichem Zustand oder im Notfall betätigen	NOT-AUS, Einleitung von NOT-AUS-Funktionen, bedingt für STOP/AUS
GELB	Anomal	Bei anomalem Zustand betätigen	Eingriff, um anomalen Zustand zu unterdrücken, Eingriff, um einen unterbrochenen automatischen Ablauf wieder zu starten
GRÜN	Normal	Betätigen, um normale Zustände einzuleiten	START/EIN hierfür jedoch bevorzugt WEISS
BLAU	Zwingend	Bei Zustand betätigen, der zwingende Handlung erfordert	Rückstellfunktion
WEISS	Keine spezielle Bedeutung zugeordnet	Für allgemeine Einleitung von Funktionen außer NOT-AUS (siehe auch Anmerkung)	START/EIN (bevorzugt), STOP/AUS
GRAU			START/EIN, STOP/AUS
SCHWARZ			START/EIN, STOP/AUS (bevorzugt)
Anmerkung: Wird eine zusätzliche Maßnahme der Kennzeichnung (z. B. Struktur, Form, Lage) zum Kennzeichnen von Drucktaster-Bedienteilen verwendet, dürfen dieselben Farben WEISS, GRAU oder SCHWARZ für verschiedene Funktionen verwendet werden, z. B. WEISS für START/EIN- und STOP/AUS-Bedienteile.			

Farben für Drucktaster und ihre Bedeutung nach EN 60204-1 (VDE 0113 Teil 1)

Farbe	Bedeutung	Erklärung	Handlung durch den Bediener	Anwendungsbeispiele
ROT	Notfall	Gefährlicher Zustand	Sofortige Handlung, um auf gefährlichen Zustand zu reagieren (z. B. durch Betätigen des NOT-AUS)	Druck/Temperatur außerhalb sicherer Grenzen, Spannungsabfall, Spannungszusammenbruch, Überfahren einer Stopp-Position
GELB	Anormal	Anormaler Zustand Bevorstehender kritischer Zustand	Überwachen und/oder Eingreifen (z. B. durch Wiederherstellen der beabsichtigten Funktion)	Druck/Temperatur übersteigt normale Bereiche, Auslösen einer Schutzeinrichtung
GRÜN	Normal	Normaler Zustand	Optional	Druck/Temperatur innerhalb normaler Bereiche, Ermächtigung fortzufahren
BLAU	Zwingend	Anzeige eines Zustandes, der Handlung durch den Bediener erfordert	Zwingende Handlung	Anweisung, vorgegebene Werte einzugeben
WEISS	Neutral	Andere Zustände: darf verwendet werden, wenn Zweifel über die Anwendung von ROT, GELB, GRÜN oder BLAU bestehen	Überwachen	Allgemeine Informationen

Farben für Leuchtmelder und ihre Bedeutung nach EN 60204-1 (VDE 0113 Teil 1)

Kennzeichnung von Leitungen

Im vorangegangenen Kapitel ist die farbige Codierung von Schaltern, Tastern und Leuchtmeldern behandelt worden. Bei der Kennzeichnung von Leitern sind durch die Norm EN 60204-1 größere Spielräume erlaubt. Sie schreibt nämlich vor, dass die "... Leiter an jeden Anschluss in Übereinstimmung mit der technischen Dokumentation identifizierbar sein müssen ...".

Die Nummerierung von Klemmen in Übereinstimmung mit dem Schaltplan genügt, wenn die Leitung visuell leicht verfolgbar ist. Bei umfangreichen Steuerungen empfiehlt es sich, sowohl den Leiter der Innenverdrahtung als auch den nach außen abgehenden Leiter so zu kennzeichnen, dass man nach dem Lösen später den Draht wieder an die richtige Klemme bringen kann. Es ist auch dort zu empfehlen, wo die Leiter für den Transport aufgetrennt werden müssen.

Mit der Formulierung in IEC 60204-1 1997, Absatz 13.2 Aderkennzeichnung, wollte das Normenkomitee folgende Punkte zum Ausdruck bringen:

1. Jeder einzelne Leiter muss identifizierbar sein, jedoch in dieser Absolutheit nur im Zusammenhang mit der Dokumentation. Es ist nicht gefordert, dass jeder Leiter für sich, ohne Dokumentation identifizierbar sein muss.
2. Die Art der Kennzeichnung und damit auch die Identifizierungsmethode sollte gegebenenfalls zwischen Hersteller und Betreiber vereinbart werden.

Es ist nicht Absicht der Norm, eine bestimmte Kennzeichnungsart zwingend weltweit vorzuschreiben. Aus Sicherheitsgründen können z. B. werksinterne Festlegungen eine höhere Priorität haben, um in Bereichen, die von demselben Personal betreut werden, Verwechslungen vorzubeugen. Diese Festlegungen können wegen des großen Geltungsbereiches der vorliegenden Norm von kleinen Einzelmaschinen (Massenprodukte) bis zu großen komplexen maschinellen Anlagen (Unikate) nicht verallgemeinert werden.

Primär muss die Sicherheit vor Montagefehlern durch entsprechende Prüfungen sichergestellt sein.

Es soll eine einheitliche Farbkennzeichnung der Leitungen verwendet werden. Folgende Farbzuordnung wird empfohlen:

- Schwarz für Hauptstromkreise für Wechsel- und Gleichstrom
- Rot für Steuerstromkreise für Wechselstrom
- Blau für Steuerstromkreise für Gleichstrom
- Orange für Verriegelungsstromkreise, die von einer externen Stromquelle versorgt werden.

Entschließt man sich zu einer reinen Farbkennzeichnung, so wird die obige Farbzuordnung empfohlen. Bindend vorgeschrieben ist lediglich die Farbe von Schutzleiter und Neutralleiter. Für alle anderen Leiter kann frei zwischen den in 14.2.4 aufgelisteten Methoden gewählt werden (Farbe, Ziffern oder Buchstaben; oder eine Kombination aus Farbe und Ziffern oder Farbe und Buchstaben).

Kennzeichnung des Schutzleiters

Der Schutzleiter muss durch Form, Anordnung, Kennzeichnung oder Farbe deutlich zu erkennen sein. Wenn Kennzeichnung nur durch Farbe erfolgt, dann muss es die Zweifarben-Kombination Grün/Gelb sein, die sich über die gesamte Leiterlänge erstrecken muss. Die Farbkennzeichnung Grün/Gelb ist ausschließlich dem Schutzleiter vorbehalten.

Kennzeichnung des Neutralleiters

Enthält ein Stromkreis einen farblich gekennzeichneten Neutralleiter, muss die Farbe Hellblau verwendet werden. Hellblau darf nicht zur Kennzeichnung von anderen Leitern verwendet werden, wenn die Gefahr der Verwechslung besteht.

Fehlt ein Neutralleiter, darf ein hellblauer Leiter für andere Zwecke verwendet werden, aber nicht als Schutzleiter.

2.2.5 Auswahl der Geräte und Grundlagen der geforderten Eigenschaften

Sicherheitsfunktion

Risikominderung mit Mitteln der PLT erfolgt dadurch, dass für jedes mögliche gefährliche Ereignis oder jeden möglichen gefährlichen Zustand einer Anlage Funktionen definiert werden, die das Eintreten des gefährlichen Ereignisses verhindern. Diese so genannten "Sicherheitsfunktionen" dienen dazu, einen sicheren Zustand der Anlage zu erhalten bzw. wieder herzustellen, wenn auf Grund eines Fehlers oder einer Störung in der Anlage ein gefährliches Ereignis einzutreten droht. Die Sicherheitsfunktion kann auch dazu dienen, das Ausmaß des Schadens aufgrund eines gefährlichen Ereignisses zu verringern.

Die Definition einer Sicherheitsfunktion umfasst immer die Spezifikation der Funktion selbst (z. B. Sperren des Zuflusses zu einem Behälter, wenn der Füllstand die Höchstgrenze erreicht hat) und die aus der Risikoanalyse abgeleitete "Safety Integrity (SIL)".

Safety Integrity Level	Betrieb im häufigen Anforderungs- oder kontinuierlichen Modus (Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde)	Betrieb im geringen Anforderungsmodus (Mittlere Wahrscheinlichkeit des Versagens der vorgesehenen Funktion bei Anforderung)
4	$\geq 10^{-9}$ ... $<10^{-8}$	$\geq 10^{-5}$ ... $<10^{-4}$
3	$\geq 10^{-8}$ ... $<10^{-7}$	$\geq 10^{-4}$ ... $<10^{-3}$
2	$\geq 10^{-7}$ ... $<10^{-6}$	$\geq 10^{-3}$ ... $<10^{-2}$
1	$\geq 10^{-6}$ ... $<10^{-5}$	$\geq 10^{-2}$ ... $<10^{-1}$

Safety Integrity Levels gemäß IEC 61508: Zielmaß der Versagenswahrscheinlichkeit einer Sicherheitsfunktion, die einem sicherheitsrelevanten System zugeordnet ist

Realisierung der Sicherheitsfunktionen

Jede Sicherheitsfunktion umfasst immer die ganze Kette, von der Informationserfassung über die Informationsauswertung bis hin zur Durchführung der beabsichtigten Aktion.

Die daran beteiligten Geräte wie z. B. fehlersichere SPS, Sensoren und Aktoren usw. müssen in ihrer Gesamtheit den bei der Risikobewertung ermittelten SIL erfüllen. Wird ein Gerät zugleich für verschiedene Sicherheitsfunktionen verwendet, hat es den höchsten SIL der einzelnen Funktionen zu erfüllen.

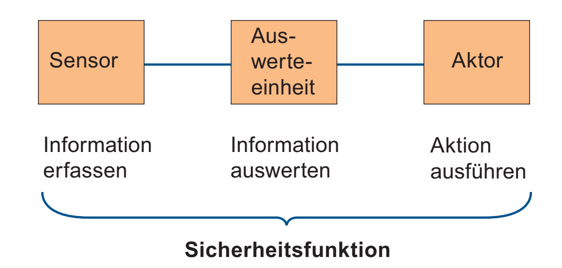


Bild 2-6 Auswerteeinheit, z. B. Sicherheits-SPS

Geräteeigenschaften

Werden für die Informationsverarbeitung SPS eingesetzt, müssen diese als "Sicherheits-SPS" (SSPS) die Anforderungen der relevanten Normen (z. B. IEC 61508), entsprechend dem angegebenen SIL, erfüllen und sollten von einem unabhängigen Prüfer zertifiziert sein. Die wesentlichen Eigenschaften einer fehlersicheren SPS, die in den Normen in abgestuftem Umfang gefordert werden, sind:

- Bei Entwicklung, Herstellung und Wartung sind bestimmte Maßnahmen und Verfahren anzuwenden, damit systematische Fehler vermieden werden.
- Die SPS muss in der Lage sein, systematische Fehler, die während des Betriebes wirksam werden, zu beherrschen.
- Die SPS muss zufällige Hardwareausfälle während des Betriebes erkennen und beherrschen können.
- Fehlerbeherrschung bedeutet, dass das System bei Erkennen eines Fehlers so reagiert, dass eine für diesen Fall festgelegte Sicherheitsfunktion (z. B. Abschalten der Anlage) zuverlässig ausgeführt wird.

Ähnliche Anforderungen gelten auch für komplexe Feldgeräte. Details dazu beschreibt IEC 61511.

Anwendung

Bei der Anwendung einer fehlersicheren SPS müssen die in dem zugehörigen Sicherheitshandbuch festgelegten Bedingungen und ggf. zusätzliche Auflagen des Zertifikates eingehalten werden.

Für die anzuschließenden Peripheriegeräte (z. B. Sensoren und Aktoren) sind zusätzlich die Anforderungen in den Normen (IEC 61508 bzw. IEC 61511) hinsichtlich folgender Aspekte zu beachten:

- Vermeiden systematischer Fehler wie z.B. Projektierungs-, Montage- und Handhabungsfehler.
- Aufdecken und Beherrschen zufälliger Fehler (Ausfälle).
- Notwendige Fehlertoleranz. Diese ist abhängig von dem Anteil der Ausfälle, die in eine sichere Richtung gehen.
- Erforderliche Wartung (wiederkehrende Prüfung).

IEC 61511 begrenzt den maximal zulässigen SIL, für den Feldgeräte eingesetzt werden dürfen, abhängig von deren Fehlertoleranz. Die in der folgenden Tabelle angegebene Fehlertoleranz kann um 1 vermindert werden, wenn:

- Die Geräte betriebsbewährt sind
- Die Geräte nur die Einstellung prozessbezogener Parameter ermöglichen
- Die Einstellung der prozessbezogenen Parameter geschützt ist

Um bei bestimmten Anwendungen die für deren SIL notwendige höhere Hardware-Fehlertoleranz zu erreichen, können Feldgeräte redundant betrieben werden, sofern die Geräte aufgrund ihrer übrigen Eigenschaften für diesen SIL geeignet sind.

Um Fehler in den Peripheriegeräten aufzudecken, können in der SSPS Test- und Überwachungsfunktionen integriert werden. Eine ggf. erforderliche Reaktion muss dabei innerhalb einer ausreichend kurzen Zeit erfolgen.

SIL	Mindest-Hardware-Fehlertoleranz, wenn die Hauptausfallrichtung in den sicheren Zustand gerichtet ist
1	0
2	1
3	2
Hinweis: Als "sicher" werden solche Ausfälle bezeichnet, bei denen ein sicherer Anlagenzustand erhalten bleibt. Hinweis: Eine Fehlertoleranz von N bedeutet, dass N+1 Fehler zum Versagen der Funktion führen.	

Maximal zulässiger SIL für Feldgeräte, abhängig von deren Fehlertoleranz

Diese Zeitanforderungen sind abhängig von der Fehlertoleranz. Die genauen Anforderungen sind in IEC 61511 definiert.

Bei der Anwendung komplexer Peripheriegeräte (z. B. Transmitter mit Mikroprozessor) ist darauf zu achten, dass diese Geräte selbst die relevanten Normen (EN 61508 bzw. IEC 61511) erfüllen.

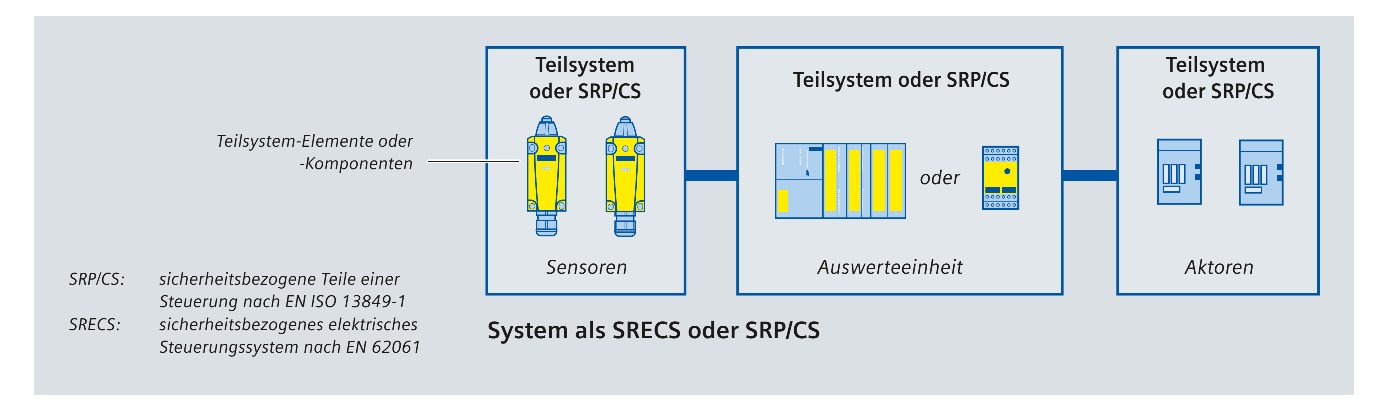
Die gesamte PLT-Schutzeinrichtung ist so zu gestalten, dass sie für alle sicherheitsrelevanten Funktionen die gültigen Normen erfüllt. Bezüglich funktionaler Sicherheit sind das EN 61508 bzw. IEC 61511.

2.3 Aufbau der Sicherheitsfunktion und Bestimmung der Sicherheitsintegrität

Innerhalb beider Sicherheitsnormen EN 62061 und EN ISO 13849-1 wird zwar eine unterschiedliche Methodik zur Bewertung einer Sicherheitsfunktion angewendet, die Ergebnisse lassen sich dennoch ineinander überführen. Beide Normen verwenden ähnliche Begriffe und Definitionen.

Die Betrachtung der gesamten Sicherheitskette beider Normen ist vergleichbar:
Eine Sicherheitsfunktion wird als System bezeichnet.

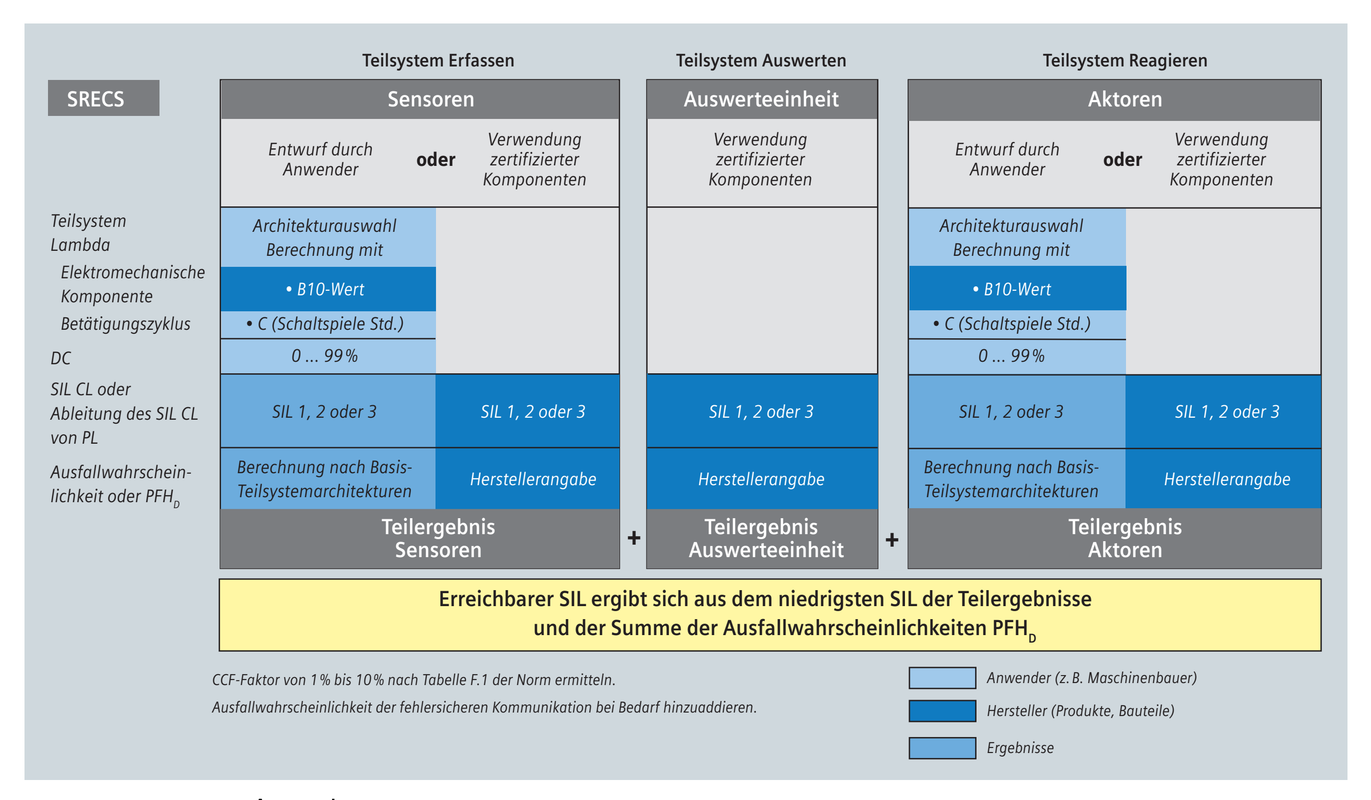
Aufbau einer Sicherheitsfunktion



Gemeinsame und vereinfachte Vorgehensweise

1. Jedes Teilsystem bzw. SRP/CS bewerten und "Teilergebnisse" erhalten. Hierzu gibt es zwei Möglichkeiten:
   - Verwendung zertifizierter Komponenten mit Herstellerangaben (z. B. SIL CL, PFH_D oder PL).
   - Auf Basis der ausgewählten Architektur (ein- oder zweikanalig) erfolgt die Berechnung der Ausfallraten der Teilsystem-Elemente oder -Komponenten. Anschließend erfolgt die Berechnung der Ausfallwahrscheinlichkeit des Teilsystems oder der SRP/CS.
2. Die Teilergebnisse bzgl. der strukturellen Anforderungen (SIL CL bzw. PL) beurteilen und die Ausfallwahrscheinlichkeiten/PFH_D addieren.

2.3.1 Methodik nach EN 62061



Anmerkung:
Eine genaue Vorgehensweise zur Bestimmung der Sicherheitsintegrität finden Sie im Funktionsbeispiel zur EN 62061. Siehe hierzu auch:
http://support.automation.siemens.com/WW/view/de/2399647

Teilsystem "Erfassen" – Sensoren

Bei zertifizierten Komponenten liefert der Hersteller die notwendigen Werte (SIL CL und PFH). Bei Verwendung von elektromechanischen Komponenten im Anwenderentwurf können SIL CL und PFH-Wert ermittelt werden.

Bestimmung des SIL CL

Für das Beispiel kann SIL CL 3 angenommen werden, da die verwendete Architektur PL x nach ISO 13849-1 entspricht und entsprechende Diagnose vorhanden ist.

Berechnung der Ausfallraten λ der Teilsystem-Elemente "Positionsschalter"

Mit dem B10-Wert und den Schaltspielen C kann mit einer Formel gemäß Abschnitt 6.7.8.2.1 der EN 62061 die gesamte Ausfallrate λ einer elektromechanischen Komponente berechnet werden.

Die Ausfallrate λ setzt sich aus ungefährlichen (λ_S) und gefahrbringenden (λ_D) Anteilen zusammen.

Berechnung der gefahrbringenden Ausfallwahrscheinlichkeit PFH_D nach verwendeter Architektur

Die EN 62061 definiert vier Architekturen für Teilsysteme (Basis-Teilsystemarchitektur A bis D). Für die Ermittlung der Ausfallwahrscheinlichkeit PFH_D stellt die Norm für jede Architektur Berechnungsformeln zur Verfügung.

Teilsystem "Auswerten" – Auswerteeinheit

Bei zertifizierten Komponenten liefert der Hersteller die notwendigen Werte.

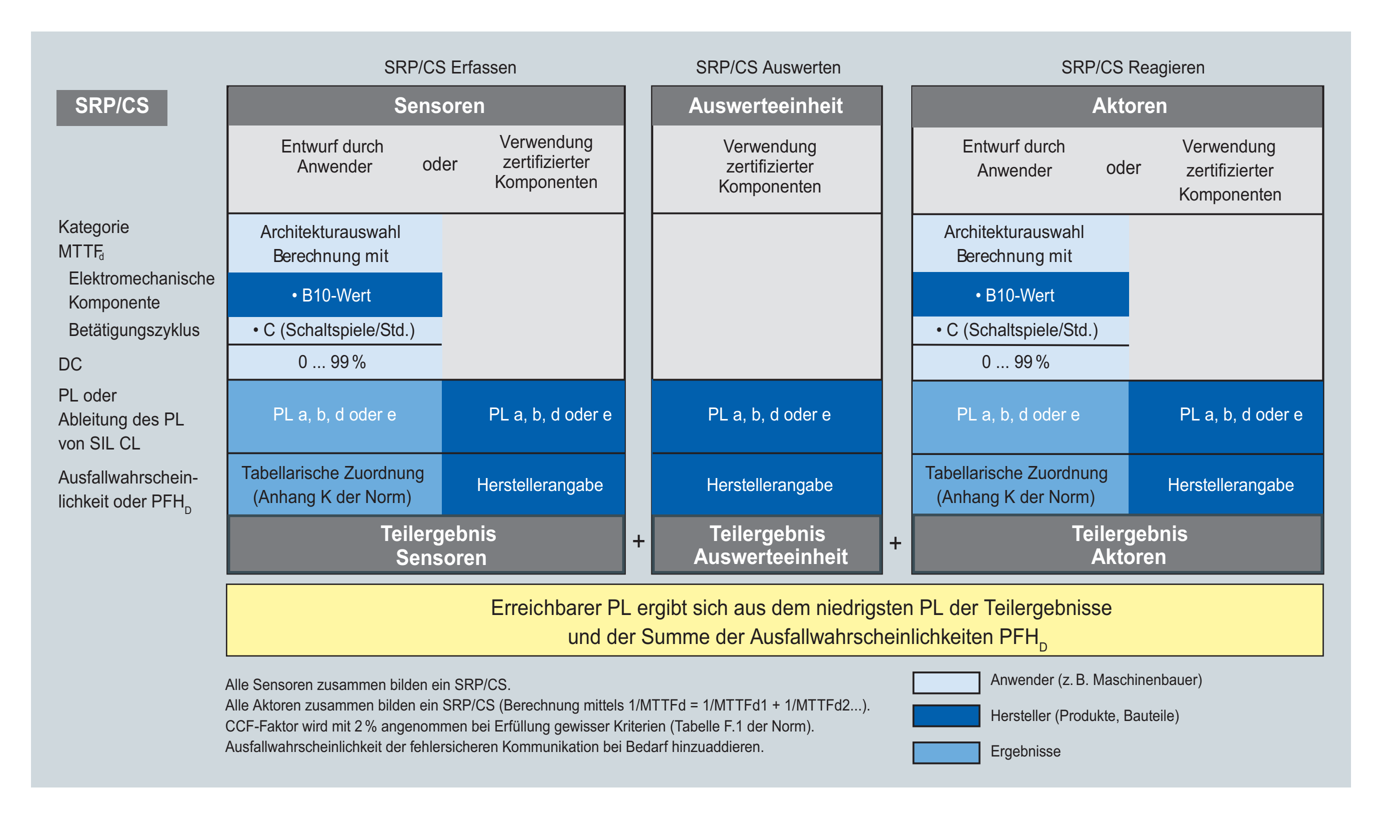
Teilsystem "Reagieren" – Aktoren

Bei zertifizierten Komponenten liefert der Hersteller die notwendigen Werte:
Bei Entwurf durch Anwender für Teilsystem "Reagieren" wird mit der gleichen Vorgehensweise gearbeitet wie beim Teilsystem "Erfassen".

Bestimmung der Sicherheitsintegrität der Sicherheitsfunktion

Es muss die kleinste SIL-Anspruchsgrenze (SIL CL) aller Teilsysteme der sicherheitsbezogenen Steuerungsfunktion (SRCF) bestimmt werden.

2.3.2 Methodik nach EN ISO 13849-1



SRP/CS "Erfassen" – Sensoren

Bei zertifizierten Komponenten liefert der Hersteller die notwendigen Werte (PL ,SIL CL oder PFH_D). Der SIL CL und der PL können auf Basis der Ausfallwahrscheinlichkeiten ineinander überführt werden, siehe Punkt Umsetzung von SIL und PL.

Bei Verwendung von elektromechanischen Komponenten im Anwenderentwurf können PL und PFH_D-Wert wie folgt ermittelt werden.

Berechnung der Ausfallraten der SRP/CS-Elemente

Mit dem B10-Wert und dem Schaltspiel n_{op} kann der Anwender die Ausfallrate $MTTF_d$ der elektromechanischen Komponente berechnen, z. B.:

$MTTF_d = B10_d/(0{,}1 * n_{op}) = 0{,}2 * 10^8$ Stunden = 2 300 Jahre entspricht $MTTF_d$ = hoch
mit n_{op} = Betätigungen pro Jahr (Angabe des Anwenders)
$n_{op} = (d_{op} * h_{op} * 3\,600\ s/h) / t_{Zyklus}$

mit folgenden Annahmen, die in Bezug zur Anwendung des Bauteils getroffen worden sind:

- h_{op} ist die mittlere Betriebszeit in Stunden je Tag
- d_{op} ist die mittlere Betriebszeit in Tagen je Jahr
- t_{Zyklus} ist die mittlere Zeit zwischen dem Beginn zweier aufeinander folgender Zyklen des Bauteils (z. B. Schalten eines Ventils) in Sekunden je Zyklus

SRP/CS "Auswerten" – Auswerteeinheit

Bei zertifizierten Komponenten liefert der Hersteller die notwendigen Werte.

SRP/CS "Reagieren" – Aktoren

Bei zertifizierten Komponenten liefert der Hersteller die notwendigen Werte.

Bei Entwurf durch Anwender für SRP/CS "Reagieren" wird mit der gleichen Vorgehensweise gearbeitet wie beim SRP/CS "Erfassen".

Bestimmung der Sicherheitsintegrität der Sicherheitsfunktion

Es muss der kleinste PL aller SRP/CS der sicherheitsbezogenen Steuerungsfunktion (SRCF) bestimmt werden.

2.3.3 Validierung auf Basis des Safety Plans

Bei der Validierung wird überprüft, ob das Sicherheitssystem (SRECS) die in der "Spezifikation der SRCF" beschriebenen Anforderungen erfüllt. Grundlage ist dabei der Sicherheitsplan.

Folgende Vorgehensweise wird bei der Validierung gefordert:

- Die Verantwortlichkeiten sind zu definieren und zu dokumentieren
- Auch alle Tests müssen dokumentiert werden
- Jede SRCF muss durch Test und/oder Analyse validiert werden
- Die systematische Sicherheitsintegrität des SRECS muss ebenfalls validiert werden

Planen

Der Sicherheitsplan ist zu erstellen. Die Validierung wird an Hand dieses Dokumentes durchgeführt.

Testen/Prüfen

Es müssen alle Sicherheitsfunktionen gemäß der Spezifikation – wie in Schritt 1 beschrieben – geprüft werden.

Dokumentation

Die Dokumentation ist ein wesentlicher Bestandteil der Begutachtung im Schadensfall. Der Inhalt der Dokumentationsliste ist durch die Maschinenrichtlinie vorgegeben. Im Wesentlichen gehören hierzu:

- Gefährdungsanalyse
- Gefährdungsbewertung
- Spezifikation der Sicherheitsfunktionen
- Hardwarekomponenten, Zertifikate etc.
- Schaltpläne
- Testergebnisse
- Software-Dokumentation inklusive Signaturen, Zertifikaten etc.
- Informationen zum Gebrauch inklusive Sicherheitshinweisen und Einschränkungen für den Betreiber

Nach erfolgreicher Validierung kann die CE-Konformitätserklärung bezüglich der risikomindernden Schutzmaßnahme erstellt werden.

2.4 Gesetzliche Anforderungen und Standard zur Sicherheit am Arbeitsplatz in Nordamerika

Hinweis: Die folgende Beschreibung soll einen Überblick über die Prinzipien und grundlegenden Anforderungen vermitteln. Sie darf nicht als vollständige Beschreibung betrachtet werden. Der Leser muss sich zusätzlich über die genauen Anforderungen sowie nationalen und lokalen Regeln für seine spezielle Anwendung informieren.

Ein wesentlicher Unterschied bei den gesetzlichen Anforderungen zur Sicherheit am Arbeitsplatz zwischen Nordamerika und Europa ist, dass es in Amerika keine einheitliche Bundesgesetzgebung zur Maschinensicherheit gibt, welche die Verantwortlichkeit des Herstellers/Lieferers abdeckt. Vielmehr besteht die generelle Anforderung, dass der Arbeitgeber einen sicheren Arbeitsplatz bieten muss.

2.4.1 USA allgemein

Die Anforderung, dass der Arbeitgeber einen sicheren Arbeitsplatz bieten muss, ist mit dem Occupational Safety and Health Act (OSHA) von 1970 geregelt.

Die Anforderungen aus dem OSH Act werden durch die Occupational Safety and Health Administration (ebenfalls als OSHA bezeichnet) verwaltet. OSHA setzt regionale Inspektoren ein, die prüfen, ob die Arbeitsplätze die gültigen Regeln erfüllen.

Die für Arbeitssicherheit relevanten Regeln der OSHA sind in OSHA 29 CFR 1910.xxx ("OSHA Regulations (29 CFR) PART 1910 Occupational Safety and Health") beschrieben (CFR: Code of Federal Regulations).

Weitere Informationen finden Sie im Internet (www.osha.gov).

2.4.2 Maschinensicherheit

Mindestanforderungen der OSHA

Die OSHA Regeln unter 29 CFR 1910 enthalten allgemeine Anforderungen für Maschinen (1910.121) und eine Reihe spezifischer Anorderungen für bestimmte Maschinentypen.

Die OSHA Regeln beschreiben Mindestanforderungen zur Gewährleistung sicherer Arbeitsplätze. Sie sollen aber Arbeitgeber nicht daran hindern, neue innovative Methoden, z. B. "state of the art" Schutzsysteme anzuwenden, um die Sicherheit der Arbeitnehmer zu maximieren.

OSHA verlangt im Zusammenhang mit bestimmten Anwendungen, dass alle elektrischen Geräte, die zum Schutz der Arbeitnehmer eingesetzt werden, von einem von OSHA genehmigten Nationally Recognized Testing Laboratory (NRTL) für die vorgesehene Anwendung genehmigt werden.

Anwendung weiterer Normen

Neben den OSHA Regeln ist es wichtig, die aktuellen Normen von Organisationen wie NFPA und ANSI sowie die in USA bestehende umfassende Produkthaftung zu beachten. Durch die Produkthaftung werden Hersteller und Betreiber im eigenen Interesse zur sorgfältigen Einhaltung von Vorschriften und zur Erfüllung des Standes der Technik "gezwungen".

Haftpflichtversicherungen verlangen im Allgemeinen, dass ihre Versicherungsnehmer die anwendbaren Standards der Standardisierungsorganisationen erfüllen. Selbstversicherte Unternehmen haben diese Anforderung zunächst nicht, müssen aber im Falle eines Unfalles nachweisen, dass sie die allgemein anerkannten Sicherheitsprinzipien angewendet haben.

Zwei besonders wichtige Sicherheitsnormen in der Industrie sind NPFA 70 (bekannt als National Electric Code (NEC)) und NFPA 79 (Electrical Standard for industrial Machinery). Beide beschreiben die grundlegenden Anforderungen an die Eigenschaften und die Ausführung der elektrischen Ausrüstung. Der National Electric Code (NFPA 70) gilt vorrangig für Gebäude, aber auch für die elektrischen Verbindungen von Maschinen und Teilmaschinen. NFPA 79 gilt für Maschinen. Damit besteht ein Graubereich in der Abgrenzung zwischen beiden Normen bei großen Maschinen, die aus Teilmaschinen bestehen. Beispielsweise können große Fördersysteme als Teil des Gebäudes betrachtet werden, so dass NFPA 70 und/oder NFPA 79 anzuwenden sind.

NFPA 79

Diese Norm gilt für die elektrische Ausrüstung von Industriemaschinen mit Nennspannungen kleiner 600 V. (Als eine Maschine wird auch eine Gruppe von Maschinen, die koordiniert zusammenarbeiten, betrachtet.) Die Neufassung NFPA 79 - 2007 enthält grundlegende Anforderungen für programmierbare Elektronik und Feldbusse, wenn diese zur Ausführung sicherheitsrelevanter Funktionen eingesetzt werden. Bei Erfüllung dieser Anforderungen dürfen besonders qualifizierte elektronische Steuerungen und Feldbusse auch für Not-Halt Funktionen der Stop Kategorien 0 und 1 verwendet werden (siehe NFPA 79 - 2007 9.2.5.4.1.4).

Die Kernanforderungen an programmierbare Elektronik und Busse sind:
Systemanforderungen (siehe NFPA 79 - 2007 9.4.3)

- Steuerungssysteme, die Software basierte Controller enthalten, müssen,

  (1) falls ein einzelner Fehler auftritt,

  - zum Abschalten des Systems in einen sicheren Zustand führen
  - Wiederanlauf verhindern bis der Fehler beseitigt ist
  - unerwarteten Anlauf verhindern

  (2) vergleichbaren Schutz wie festverdrahtete Steuerungen bieten

  (3) entsprechend einem anerkannten Standard, der Anforderungen für solche Systeme definiert, ausgeführt sein.

Als geeigneter Standard wird IEC 61508 in einer Note genannt.

Anforderungen an programmierbare Betriebsmittel (siehe NFPA 79 - 2007 9.4.3.4.1) sind:

- Software und Firmware basierte Controller, die in sicherheitsrelevanten Funktionen eingesetzt werden, müssen für solche Anwendung gelistet sein (d.h. durch ein NRTL zertifiziert sein). In einer Note wird gesagt, dass IEC 61508 Anforderungen zum Design solcher Controller liefert.

"Listing"-Dateien elektronischer Geräte für Sicherheitsfunktionen

Zur Umsetzung der Anforderung in der NFPA 79: 2007 hat UL eine spezielle Kategorie für "Programmable Safety Controllers" (Bezeichnungscode NRGF) definiert. Diese Kategorie behandelt Steuerungsgeräte, die Software beinhalten und zur Anwendung in Sicherheitsfunktionen vorgesehen sind. NFPA 79 ist in Bearbeitung und es wird aktiv am nächsten planmäßigen Update gearbeitet, das 2011 kommen soll. Unter Berücksichtigung der Funktionssicherheit und für den Einsatz neuer Technologien, wie z. B. kabellose Hängebedienungstafel einschließlich elektronischer Abschaltgeräte, sollte man die EN ISO 13849-1, 2006 betrachten.

Die genaue Beschreibung der Kategorie sowie die Liste der Geräte, die diese Anforderung erfüllen, sind im Internet zu finden:

www.ul.com (http://www.ul.com) –> certifications directory –> UL Category code / Guide information –> search for category "NRGF"

TÜV Rheinland of North America, Inc. ist ebenfalls NRTL für diese Anwendungen. Die dort gelisteten Produkte können auch im Internet angezeigt werden: Von der Homepage aus kann mit der "ID" des Gerätes (Enter TUVdot-COM ID) die im Listing eingetragene Beschreibung abgerufen werden.

ANSI B11

Die ANSI B11-Normen sind gemeinsame Standards/Normen, die von Gremien wie z. B. der Association for Manufacturing Technology (AMT – Vereinigung für Fertigungstechnologien), National Fire Protection Association (NFPA – Staatlicher Brandschutzverband) und der Robotic Industries Association (RIA - Roboterindustrieverband) entwickelt wurden.

Mit Hilfe der Risikoanalyse werden die Gefahren einer Maschine bewertet. Risikoanalyse ist eine wichtige Anforderung gemäß NFPA 79 - 2007, ANSI/RIA 15.06 1999, ANSI B11.TR-3 und TR-4 und SEMI S10 (Halbleiter). Mit Hilfe der dokumentierten Ergebnisse einer Risikoanalyse kann die geeignete Sicherheitstechnik ausgewählt werden, basierend auf der gegebenen Sicherheitsklasse der jeweiligen Anwendung.

Die aktuellen Listen der ANSI-Normen finden Sie nachstehend. Sie dienen als Referenz, und falls eine genehmigte Überarbeitung diese ablösen sollte, so gilt die überarbeitete Norm.

2.4.3 Prozessindustrie in den USA

Die grundlegenden Sicherheitsanforderungen der OSHA für die Prozessindustrie sind in OSHA´s Process Safety Management of Highly Hazardous Chemicals, Explosives and Blasting Agents Standard (PSM), 29 CFR 1910.119 beschrieben (www.osha.gov).

Guidelines dazu gibt OSHA mit: CPL 22.45A "Process Safety Management of Highly Hazardous Chemicals - Compliance Guidelines and Enforcement Procedures.

OSHA verlangt, dass die Prozessinstrumentierung gemäß anerkannter und allgemein akzeptierter "good engineering practice" ausgeführt wird. Mit Schreiben vom März 2000 stellt OSHA auf eine entsprechende Anfrage von ISA klar, dass ANSI/ISA 84.01 ein Standard mit nationaler Übereinstimmung ist und von OSHA als allgemein akzeptierte "good engineering practice" anerkannt wird. Mit dem selben Schreiben stellt OSHA aber auch klar, dass ISA 84.01 nicht grundsätzlich als der einzige Standard zum Erfüllen der Anforderungen von 1910.119 (PSM) betrachtet wird.

Aus CFR 1910.119 geht zunächst nicht klar hervor, ob die Anforderungen sich auf die vollständige Instrumentierung beziehen. In der Prozessindustrie sind zwei Typen der Instrumentierung üblich. "Safety Instrumented Systems" (SIS) und "Basic Process Control System" (BPCS). ANSI/ISA 91.01 definiert, dass nur das SIS unter den OSHA Regeln zu behandeln ist.

IEC 61511 "Functional safety: Safety Instrumented Systems for the process industry sector" ist der IEC Standard mit dem gleichen Umfang wie ISA 84.01. Er wurde unter starker Beteiligung von ISA entwickelt und soll als Neufassung der ISA 84 übernommen werden.

Ein großer Teil von Prozessen ist im Umfang von ISA 84.01, fällt aber formal nicht unter 29 CFR 1910.119 (PSM). Auch hier sollte der Standard angewendet werden, um nicht die grundsätzlichen Anforderungen des "Duties" Abschnittes des Occupational Safety and Health Act (OSHA) zu verletzen.

2.4.4 Arbeitsschutzbestimmungen und Sicherheitsnormen in Kanada

Das Kanadische Arbeitsgesetzbuch (Canada Labour Code)

Das Kanadische Arbeitsgesetzbuch ist das für alle Industriezweige Kanadas gültige Gesetz. Teil 2 des Kanadischen Arbeitsgesetzbuches befasst sich mit der Sicherheit und dem Gesundheitsschutz am Arbeitsplatz. Nach der kanadischen Verfassung sind in erster Linie die Provinzbehörden für das Arbeitsrecht zuständig. Im Arbeitsschutzgesetz (Occupational Health and Safety Act, OHSA) werden die Rechte und Pflichten aller betrieblichen Parteien festgelegt. Sein Hauptzweck ist der Schutz der Arbeitnehmer vor Gesundheits- und Sicherheitsrisiken bei der Arbeit. Das OHSA setzt Verfahren für den Umgang mit Risiken am Arbeitsplatz fest. Wird das Gesetz nicht freiwillig erfüllt, sieht es dessen Vollstreckung vor. Die kraft dem OHSA erlassenen Verordnungen beinhalten bestimmte Anforderungen, Normen und Verfahrensweisen, die zur Verringerung der Gefahr von Arbeitsunfällen einzuhalten sind.

Von der Bundes- bzw. den Provinz- oder Gebietsregierungen bestellte Beamte sind dazu befugt, Arbeitsplätze zu besichtigen. Darüber hinaus können sie den Vollzug des Gesetzes durch sämtliche erforderliche Vollzugsmittel erwirken, die sich an Arbeitgeber und Arbeitnehmer richten. Hierzu gehören auch Anordnungen zur Arbeitseinstellung, Geldstrafen und eine strafrechtliche Verfolgung. Hierzu gehören beispielsweise das Arbeitsministerium (MoL) in Ontario oder die Kommission für Gesundheit und Sicherheit bei der Arbeit (CSST) in Quebec. Die Beamten arbeiten eng mit ihren Geschäftsstellen, Verbänden für Sicherheit am Arbeitsplatz (Safe workplace associations, SWAs), Schulungszentren und Kliniken für Arbeitnehmer sowie dem Kanadischen Zentrum für Sicherheit und Gesundheitsschutz am Arbeitsplatz zusammen. Zu diesen leitenden Organisationen gehören auch der Verband zur Unfallverhütung an industriellen Arbeitsplätzen (Industrial Accident Prevention Association, IAPA) in Ontario und das Institut de Recherche Robert-Sauvé en Santé et en Sécurité du Travail (IRSST) in Quebec. Versicherungskammern spielen ebenfalls eine wichtige Rolle bei der Sicherheit am Arbeitsplatz. Beispielsweise beaufsichtigt die Versicherungskammer für Sicherheit am Arbeitsplatz (Workplace Safety and Insurance Board, WSIB) das Ausbildungs- und Schulungssystem für Sicherheit am Arbeitsplatz, zahlt Berufsunfähigkeitsrenten im Rahmen des Unfallversicherungsprogramms aus, überwacht die Qualität der Gesundheitsvorsorge durch den Einsatz finanzieller Maßnahmen usw.

Links:

- Regierung von Kanada, Sicherheit und Gesundheitsschutz am Arbeitsplatz in Kanada (www.hrsdc.gc.ca)
- Arbeitsministerium (www.gov.on.ca/lab/)
- Commission de la santé et de la sécurité du travail (www.csst.qc.ca)
- Verband zur Unfallverhütung an industriellen Arbeitsplätzen (www.iapa.on.ca)
- Das Institut de Recherche Robert-Sauvé en Santé et en Sécurité du Travail (www.irsst.qc.ca)
- Sicherheit am Arbeitsplatz & Versicherungskammer (www.wsib.on.ca)

Die Verordnung für Industrieunternehmen nach dem OHSA in Ontario, Verordnung 528/00 Abschnitt 7 (PSHSR -Pre Start Health and Safety Review, Pre-Start-Sicherheits- und Gesundheitsprüfungen) ist seit dem 7. Oktober 2000 in Kraft, wobei sich der 2. Punkt der Tabelle auf die Sicherheit von Maschinen bezieht. Der Arbeitgeber hat sicherzustellen, dass der Arbeitsplatz sämtlichen Anforderungen des OHSA sowie den Verordnungen Genüge leistet. Die Verordnung ist größtenteils eine leistungsbasierte Norm, d.h., sie bestimmt die anzuwendende Sicherheitsebene sowie das beabsichtigte Ziel, legt jedoch nicht fest wie die geforderte Sicherheitsebene zu erreichen ist.

Abschnitt 7 oder Verordnung 528/00 bezieht sich auf die gegenwärtig in Kanada geltenden Normen. Um die Anforderungen aus Abschnitt 7 vollständig zu erfüllen, muss Bezug auf andere anerkannte geltende Richtlinien und Normen genommen werden, beispielsweise die Brandschutzrichtlinien von Ontario (Ontario Fire Code), die Nationalen Brandschutzrichtlinien (National Fire code), die NFPA-Gesetze und -Normen, CSA-Gesetze und -Normen, ANSI-Normen usw. Die dargestellte Tabelle ist eine Zusammenfassung der für die Maschinensicherheitsumstände geltenden Normen. Diese werden als Hilfestellung zur Erfüllung von Abschnitt 7 der Verordnung aufgelistet.

Bei A-&-B-Normen handelt es sich um Sicherheitsgrundnormen, die grundlegende Konzepte und Richtlinien für Konstruktions- und allgemeine Aspekte vorgeben beziehungsweise sich auf einen Sicherheitsaspekt oder eine Art sicherheitsbezogener Vorrichtung beziehen, die auf Maschinen oder Prozesse angewandt werden kann.

Bei C-Normen handelt es sich um Sicherheitsnormen, die sich auf detaillierte Sicherheitsanforderungen für eine bestimmte Maschine oder einen bestimmten Prozess beziehen.

Folgendes sind die **wichtigsten Normwerke für Maschinensicherheit in Kanada**, die die Verwendung sicherheitsbezogener soft- und firmwarebasierter Steuerungen einschließlich deren neuester Änderungen anerkennen:

- CSA Z432-04 "Maschinensicherheit" erkennt die Verwendung einer programmierbaren Sicherheitssteuerung nach Abschnitt 8.3 an. Diese Norm bezieht sich auf den Schutz von Personen vor Risiken, die aus der Verwendung mobiler oder ortsfester Maschinen herrühren. Sie gibt die einzuhaltenden Kriterien sowie die Beschreibung, Auswahl und Anwendung von Schutz- und Sicherheitsvorrichtungen vor. Ist eine gegenwärtige CSA-Norm für eine bestimmte Maschinenart vorhanden, muss diese gemeinsam mit dieser Norm angewandt werden, um den bestmöglichen Schutz für diese besondere Situation zu erzielen.

Die CSA-Sicherheitsnormen erfordern die Zertifizierung der sicherheitsbezogenen soft- und firmwarebasierten Sicherheitssteuerungen durch ein landesweit anerkanntes Prüflabor (Nationally Recognized Testing Laboratory, NRTL) oder ein vom Normungsausschuss von Kanada (Standards Council of Canada, SCC) zugelassenes Prüflabor gemäß einem für Sicherheitsvorrichtungen anerkannten geltenden Standard.

2.5 Sicherheitsanforderungen für Maschinen in Japan

Zur Anwendung im Inland

Die Situation in Japan war bisher anders als in Europa und USA. Im Gegensatz zu Europa und USA, wo der Arbeitgeber für die Sicherheit am Arbeitsplatz verantwortlich ist, muss in Japan der Arbeitnehmer selber darauf achten, dass ihm nichts passiert. Es darf deshalb nur entsprechend geschultes Personal an eine Maschine.

Vergleichbare gesetzliche Anforderungen zur funktionalen Sicherheit wie in Europa existierten folglich nicht. Ebenso spielt die Produkthaftung keine solche Rolle wie in USA. Inzwischen hat man aber erkannt, dass dieses Konzept heute nicht mehr reicht. Man geht zu dem Grundprinzip wie in Europa und USA über.

Es gibt keine gesetzliche Anforderung zur Anwendung von Normen, aber eine Verwaltungsempfehlung zur Anwendung von JIS (Japanese Industrial Standards): Japan lehnt sich an das europäische Konzept an und hat die grundlegenden Normen als nationale Standards übernommen (siehe Tabelle).

ISO/IEC Nummer	JIS Nummer	Hinweis
EN ISO 12100-1	JIS B 9700-1	frühere Bezeichnung TR B 0008
EN ISO 12100-2	JIS B 9700-2	frühere Bezeichnung TR B 0009
EN ISO 14121 (EN 1050)	JIS B 9702	
EN ISO 13849-1 (Ed. 1)	JIS B 9705-1	
EN ISO 13849-2 (Ed. 2)	JIS B 9705-1	
IEC60204-1	JIS B 9960-1	ohne Annex F bzw. Route Map des europäischen Vorwortes
IEC1508-1 to 7	JIS C 0508	
IEC 62061	JIS B 9961	

Für global operierende Maschinenhersteller und -anwender

Exportorientierte japanische Maschinenhersteller haben ein dringendes Interesse, die europäischen und amerikanischen Anforderungen zu erfüllen, damit ihre Produkte den Anforderungen der Zielmärkte genügen. Firmen mit global verteilten Fertigungsstätten orientieren sich ebenfalls an den europäischen und amerikanischen Anforderungen, um möglichst einheitliche Sicherheitskonzepte in allen Fabriken zu haben.

2.6 Wichtige Adressen

2.6.1 Europa

1. CEN-Mitglieder = Bezugsquellen für nationale Fassungen von EN + prEN

AENOR	Asociación Española de Normalización y Certificación (AENOR) Génova 6 E-28004 Madrid Telefon: + 34 91 432 60 00 Telefax: + 34 91 310 31 72 E-Mail: info@aenor.es
AFNOR	Association Française de Normalisation 11 Avenue Francis de Pressensé F93571 Saint-Denis La Plaine Cedex Telefon: + 33 1 41 62 80 00 Telefax: + 33 1 49 17 90 00
AS	Austrian Standard Heinestraße 38 A-1020 Wien Telefon: + 43 1 213 00 0 Telefax: + 43 1 213 00 355 E-Mail : office@as-plus.at
BSI	British Standards Institution 389 Chiswick High Road GB-London W4 4AL Telefon: + 44 208 996 90 01 Telefax: + 44 208 996 70 01 E-Mail: cservices@bsigroup.com
CEN	European Comittee for Standardization Avenue Marnix 17 B-1000 Brussels Telefon: + 3225500811 Telefax: + 3225500819 E-Mail: infodesk@cenorm.be
CENELEC	European Comittee for Electrotechnical Standardization Avenue Marnix 17 B-1000 Brussels Telefon: + 3225196871 Telefax: + 3225196919 E-Mail: info@cenelec.eu
DIN	Deutsches Institut für Normung e.V. Burggrafenstr. 6 D-10787 Berlin Telefon: + 49 30 26 01 0 Telefax: + 49 30 26 01 12 31 E-Mail: postmaster@din.de

DS	Dansk Standard Kollegievej 6 DK-2920 Charlottenlund Telefon: + 45 39 96 61 01 Telefax: + 45 39 96 61 02 E-Mail: dansk.standard@ds.dk
ELOT	Hellenic Organization for Standardization 313, Acharnon Street GR-11145 Athens Telefon: + 30 210 21 20 100 Telefax: + 30 210 21 20 131 E-Mail: info@elot.gr
IBN/BIN	Bureau de Normalisation Rue de Birmingham 131 BE-1070 Bruxelles Telefon: + 32 2 738 01 11 Telefax: + 32 2 733 42 64
ILNAS	Institut luxembourgeois de la normalisation B.P. 10 L-2010 Luxembourg Telefon: + 352 46 97 46 1 Telefax:+ 352 22 25 24 E-Mail: info@ilnas.public.lu
IPQ	Instituto Portugues da Qualidade Rua Antonio Giao, 2 P-2829-513 Caparica Telefon: + 351 21 294 81 00 Telefax: + 351 21 294 81 01 E-Mail: ipq@mail.ipq.pt
IST	Icelandic Standards Skúlatún 2 IS-105 Reykjavik Telefon: + 354 520 71 50 Telefax: + 354 520 71 71 E-Mail: stadlar@stadlar.is
NEN	Nederlands Normalisatie-Instituut Postbus 5059 NL-2600 GB Delft Telefon: + 31 152 690 390 Telefax: + 31 152 690 190 E-Mail: info@nen.nl
NSAI	National Standards Authority of Ireland Northwood, Stantry, IRL-Dublin 9 Telefon: + 353 1 807 38 00 Telefax: + 353 1 807 38 38 E-Mail: info@nsai.ie

NSF	Norges Standardiseringsforbund P.O. Box 242 NO-1326 Lysaker Telefon: + 47 67 83 86 00 Telefax: + 47 67 83 86 01 E-Mail: info@standard.no
SFS	Suomen Standardisoimisliitto r.y. PO Box 130 FIN-00101 Helsinki Finland Telefon: + 358 9 149 93 31 Telefax: + 358 9 146 49 25 E-Mail: sfs@sfs.fi
SIS	Standardiseringen i Sverige Sankt Paulsgatan 6 S - 118 80 Stockholm Telefon: + 46 8 555 520 00 Telefax: + 46 8 555 520 01 E-Mail: info@sis.se
SNV	Schweizerische Normen-Vereinigung Burglistraße 29 CH-8400 Winterthur Telefon: + 41 52 224 54 54 Telefax: + 41 52 224 54 74 E-Mail: info@snv.ch
UNI	Ente Nazionale Italiano di Unificazione Via Sannio 2 I-20137 Milano MI Telefon: + 39 02 70 02 41 Telefax: + 39 02 70 02 43 75 E-Mail: uni@uni.com
UNMZ	Czech Office for Standards, Metrology and Testing Biskupsky dvur 5 CZ-128 01 Praha 2 Telefon: +420 224 907 175 Telefax: +420 224 915 064 E-Mail: posta@unmz.cz

2. DIN – Deutsches Institut für Normung e.V., Federführende Normenausschüsse in Bezug auf Maschinen

NAM	Normenausschuss Maschinenbau (NAM) im DIN Lyoner Str. 8 Postfach 710864 60498 Frankfurt/M. Telefon: 069/6603-1341 Telefax: 069/6603-1557
NWM	Normenausschuss Werkzeugmaschinen Corneliusstraße 4 60325 Frankfurt Telefon: 069/75608123 Telefax: 069/75608111
AGSA, FNErg, FNFW, FNL, NAL, NALS, NAS, Nasg, NI, NKT, NMP, Textilnorm	DIN Deutsches Institut für Normung e.V. 10787 Berlin Telefon: 030/2601-0 Telefax: 030/2601-1260
FNCA, FNKä, FWS, Naa, NAD, NL, NÖG, NRK, NÜA	DIN Deutsches Institut für Normung e.V. Zweigstelle Köln Kamekestraße 8 50672 Köln Telefon: 0221/5713-0 Telefax: 0221/5713-414
NA EBM	Normenausschuss Eisen-, Blech- und Metallwaren Gothaer Str. 27 40880 Ratingen Telefon: 02102/940854 Telefax: 02102/940851
NA FuO	Normenausschuss Feinmechanik und Optik Alexander-Wellendorff-Str. 2 75172 Pforzheim Telefon: 07231/918827 Telefax: 07231/918833
FAKAU	Normenausschuss Kautschuktechnik Zeppelinstr. 69 60487 Frankfurt/M. Telefon: 069/7936-0/117 Telefax: 069/7936175
DKE	Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE Stresemannallee 15 60596 Frankfurt/M. Telefon: 069/6308-0 Telefax: 069/6308-9863 E-Mail: dke@vde.com

3.Bezugsquellen für technische Regelwerke in Deutschland

Für EG-Richtlinien sowie Gesetze und Verordnungen	Bundesanzeiger-Verlags GmbH Amsterdamer Straße 192 50667 Köln Telefon: (0221) 97668-0 E-Mail: service@bundesanzeiger.de
Für DIN-Normen und VDM-Einheitsblätter	Beuth Verlag GmbH Burggrafenstraße 6 10787 Berlin Telefon: (030) 2601-0 Telefax: (030) 2601-1260
Für VDE-Vorschriften sowie Normen der DKE und IEC	VDE-Verlag GmbH Bismarckstraße 33 10625 Berlin Telefon: (030) 34 80 01-0 Telefax: (030) 34 80 01-9088 E-Mail: kundenservice@vde-verlag.de
Für Unfallverhütungsvorschriften und ZH-1-Schriften der Berufsgenossenschaften	Carl Heymanns Verlag KG Luxemburger Straße 449 50939 Köln Telefon: (0221) 94373-0 Telefax: (0221) 94373-901
Alles über Normen, Vorschriften, Richtlinien	Deutsches Informationszentrum für Technische Regeln (DITR) im DIN (Deutsches Institut für Normung) Burggrafenstraße 6 10787 Berlin Telefon: (030) 2601-0 Telefax: (030) 2628125

2.6.2 Amerika

Zusätzliche Informationen über Maschinensicherheit finden Sie unter:

ANSI (American National Standards Institute)	http://www.ansi.org
OSHA (Occupational Safety and Health Administration)	http://www.osha.gov
NFPA (National Fire Protection Association)	http://www.nfpa.org
TUV Rheinland of N.A. Inc.	http://www.us.tuv.com
UL (Underwriter Laboratories)	http://www.ul.com
CSA (Canadian Standards Association)	http://www.csa.ca
CCOHS (Canadian Center for Occupational - Health and Safety)	http://www.ccohs.ca
NIOSH (National Institute of Occupational Health and Safety)	http://www.cdc.gov/niosh/homepage.html
NSC (National Safety Council)	http://www.nsc.org
ASSE (American Society of Safety Engineers)	http://www.asse.org
RIA (Robotic Industries Association)	http://www.robotics.org

Begriffe

3

A

Begriff	Referenz	relevante Norm
AOPD/AOPDDR	Sicherheitsbauteil, BWS	ISO 12100-1
	Active optoelectronic protection device responsive to diffuse reflection Aktive optoelektronische Schutzeinrichtung.	
Aktor	zwangsgeführte Kontakte	
	Stellglied, z. B. Motor, Ventil, Signalleuchten, Relais, Motorschütze mit zwangsgeführten Kontakten usw.	
Anforderung	SRECS, SRCF	IEC 62061
	(engl.: demand) Ereignis, das das SRECS veranlasst, seine SRCF auszuführen.	
Anforderungsklasse Anforderungsrate ohne Schutzeinrichtung	Kategorien	DIN 19250 (nicht mehr gültig) IEC 61511-3
	Die Zuordnung von Anforderungen für die Realisierung der Schutzeinrichtung, die zu einer dem Risiko angemessenen sicherheitsbezogenen Leistungsfähigkeit der Einrichtung führen sollen. Die Anforderungsklasse ergibt sich aus dem Produkt des Schadensausmaßes und der Eintrittswahrscheinlichkeit (W, Wahrscheinlichkeit des unerwünschten Ereignisses). Siehe auch in der IEC 61511-3, Bild E.2 (Beziehung zwischen IEC 61511, DIN V 19250 und VDI/VDE 2180).	
Anlaufsperre	NOT-HALT (Rückstellung) Sicherheitsschaltgerät	ISO 13850
	Die Rückstellung des Befehls darf die Maschine nicht wieder in Gang setzen, sondern das Wiederingangsetzen ermöglichen (ISO 13850). Durch die Anlaufsperre wird das automatische Wiederanlaufen durch das Sicherheitsschaltgerät verhindert, wenn die Versorgungsspannung nach Unterbrechung wiederkehrt.	
Anlauftestung	Sicherheitsschaltgerät	
	Ein manueller oder automatischer Test, der durchgeführt wird, um das sicherheitsbezogene Steuerungssystem zu testen, nachdem die Versorgungsspannung an das Sicherheitsschaltgerät angelegt wurde. Ein Beispiel für eine Anlauftestung ist das manuelle Öffnen und Schließen einer trennenden Schutzeinrichtung nach dem Einschalten der Versorgungsspannung.	

Begriff	Referenz	relevante Norm
Ansteuerung (z. B. eines Schützes)	Sicherheitsschaltgerät Redundanz, Diversität	
	Einkanalige Ansteuerung (nicht redundant): Das Sicherheitsschaltgerät wird über einen einzelnen Signalgeber-Kontakt bzw. Ausgang angesteuert. **Zweikanalige Ansteuerung (redundant):** Das Sicherheitsschaltgerät wird über zwei Signalgeber-Kontakte bzw. Ausgänge angesteuert. *Anmerkung: Bei dieser Art der Ansteuerung erreicht die Sicherheitseinrichtung maximal die Kategorie 4 nach ISO 13849-1, wenn das Sicherheitsschaltgerät über eine Querschlusserkennung verfügt, wobei die zwei Signalgeber Teil einer Schutzeinrichtung (NOT-HALT Einrichtung, trennende Schutzeinrichtung) sein müssen. Wird ein zweikanaliges Sicherheitsschaltgerät einkanalig angesteuert, so muss der Signalgeber-Kontakt bzw. Ausgang beide Kanäle des Sicherheitsschaltgerätes schalten (z. B. SIRIUS 3TK28 Elektronik).*	
ANSI B11	OSHA, NFPA 79	
	Unter ANSI B11 gibt es eine Reihe weiterer Standards zur Sicherheit in der Industrie, die eine zusätzliche Anleitung zum Erzielen der geforderten Sicherheit bieten (USA).	
ASIsafe	PROFIsafe	
	Sicherheitsgerichtete Kommunikation über das Standard AS-Interface (AS-Interface Safety at Work).	
Antivalenz	Zwangsführung	
	Kontravalenz (Gegenwertigkeit): zwei unterschiedliche Signale, z. B. Öffner- und Schließer-Kontakte.	
Ansprechzeit	Sicherheitsschaltgerät	
	Zeit von der Befehlsauslösung bis zur -ausführung: z. B. Zeit vom Auslösen des Steuerkommandos (z. B. NOT-HALT) bis zum Öffnen der Kontakte der Lastschalteinrichtung bzw. bis zum vollkommenen Stillsetzen des Antriebs.	
Ausfall	Gefahr bringender Ausfall	ISO 12100-1
	(engl. "failure") Die Beendigung der Fähigkeit einer Einheit, eine geforderte Funktion zu erfüllen.	
Ausfallgrenzwert	PFH_D	IEC 62061
	(engl.: target failure value) vorgesehene PFH_D die zu erreichen ist, um die Anforderung(en) zur Sicherheitsintegrität zu erreichen.	
Ausschalten im Notfall	Stillsetzen im Notfall, Handlungen im Notfall, Notfall, Stopp-Funktion, NOT-HALT	IEC 60204-1, Anhang D (Handlungen im Notfall), ISO 12100-1, ISO 13850
	Eine Handlung im Notfall, die dazu bestimmt ist, die Versorgung mit elektrischer Energie zu einer ganzen oder einem Teil einer Installation abzuschalten, falls ein Risiko für elektrischen Schlag oder ein anderes Risiko elektrischen Ursprungs besteht. Sie soll aufkommende oder bestehende Gefahren für Personen und Schäden an der Maschine, am Arbeitsgut oder der Umwelt abwenden oder mindern. *Anmerkung: Gefahren sind u. a. funktionale Unregelmäßigkeiten, Fehlfunktionen der Maschine, nicht hinnehmbare Eigenschaften des zu bearbeitenden Materials und menschliche Fehler.*	
Auswerteeinheit	Sicherheitsschaltgerät, SRECS, SRP/CS	
	Eine sicherheitsgerichtete Auswerteeinheit erzeugt, abhängig vom Zustand angeschlossener Signalgeber entweder nach einer festen Zuordnung oder nach programmierten Anweisungen ein sicherheitsgerichtetes Ausgangssignal.	

Begriff	Referenz	relevante Norm
Automatischer Start	Start	IEC 60204-1
	Das Wiederherstellen einer Sicherheitsfunktion erfolgt automatisch (ohne Ein-Taster). Dies ist z. B. zulässig für bewegliche trennende Schutzeinrichtungen, die nicht hintergehbar oder hintertretbar sind (EN ISO 12100-2), jedoch nicht für eine Not-Halt-Einrichtung. Diese Startart ist nur zulässig nach erfolgter Gefahrenbeurteilung.	
A-Norm	harmonisierte Norm	ISO 12100-1, ISO 14121, EN 1070
	Sind europäische Grundnormen (Typ A), die in der Maschinenrichtlinie gelistet sind: Gestaltungsgrundsätze, Begriffe (ISO 12100-1, EN 1070)/Gefahrenanalyse, Risikobeurteilung (ISO 14121).	

B

Begriff	Referenz	relevante Norm
Beta β	PFH_D	IEC 62061
	Common cause failure factor (0,1 – 0,05 – 0,02 – 0,01): Faktor der Fehler gemeinsamer Ursache.	
B10	Lambda λ, PFH_D	IEC 62061
	Der B10-Wert für verschleißbehaftete Geräte wird in Anzahl Schaltspiele ausgedrückt: Dies ist die Anzahl der Schaltspiele bei der im Laufe eines Lebensdauerversuchs 10% der Prüflinge ausgefallen sind (oder: Anzahl Betätigungszyklen nach denen 10% der Geräte ausgefallen sind). Mit dem B10-Wert und dem Betätigungszyklus kann die Ausfallrate für elektromechanische Komponenten errechnet werden. **B10d** B10d = B10 / Anteil Gefahr bringender Ausfälle	
Basisgerät	Grundgerät, Erweiterungsgerät, Sicherheitsschaltgerät	ISO 13849-1
	Ersatzbegriff für Grundgerät.	
Befehlsgerät (NOT-HALT Gerät)	NOT-HALT	ISO 13850
	Ein manuell betätigtes Steuergerät, das zur Auslösung einer NOT-HALT Funktion verwendet wird.	
Betätiger	Getrennter Betätiger, Positionsschalter	
	Mehrfach kodiertes mechanisches Betätigungselement, das bei Herausziehen aus dem Positionsschalter (Kopf) die zwangsöffnenden Kontakte öffnet.	
B-Norm	harmonisierte Norm	ISO 12100-1, ISO 14121, EN 1070
	Sind europäische Gruppennormen (Typ B), die in der Maschinenrichtlinie gelistet sind: Typ B1 zu allgemeinen Sicherheitsaspekten (z. B. Ergonomie, Sicherheitsabstände EN 999) Typ B2 zu Systeme und Schutzeinrichtungen (z. B. ISO 13849-1).	
BWS	AOPD, OSSD, Laserscanner, Lichtgitter, Lichtvorhänge	IEC 61496
	Steuerungs-/Überwachungs-Funktion mit Ausgangsschaltelement, auch OSSD genannt.	
BWP	Positionsschalter	
	Berührungslos **w**irkende **P**ositionsschalter (z. B. Magnetschalter).	

C

Begriff	Referenz	relevante Norm
C-Norm	harmonisierte Norm	ISO 12100-1, ISO 14121, EN 1070
	Sind europäische Produktnormen (Typ C), die in der Maschinenrichtlinie gelistet sind: Fachnormen – spezifische Anforderungen an bestimmte Maschinen (z. B. Pressen EN 692).	
C	B10, PFH_D	IEC 62061
	Duty **C**ycle: Betätigungszyklus (pro Stunde) eines elektromechanischen Bauteils.	
CCF	Lambda λ, PFH_D	IEC 61508, IEC 62061, ISO 13849-1
	Common **c**ause **f**ailure: Ausfall in Folge gemeinsamer Ursache (z. B. Kurzschluss).	
CE	MRL, Konformitätserklärung, Kennzeichnung	MRL Art. 10-12, Anhang III (EN 45014)
	Der Maschinenhersteller muss eine CE − Kennzeichnung durchführen, wenn er die Maschine in Verkehr bringen möchte (MRL, "Schutz vor Willkür"). *Anmerkung: CE – Kennzeichnung für die Niederspannungsrichtlinie ist nicht vergleichbar mit der CE – Kennzeichnung für die Maschinenrichtlinie.*	
CEN CENELEC		
	Comité **E**uropéen de **N**ormalisation: Europäisches Komitee für Normung (Europäischer Normungsausschuss). **C**omité **E**uropéen de **N**ormalisation **Elec**trotechnique: Europäischer Normungsausschuss für Elektrotechnik.	

D

Begriff	Referenz	relevante Norm
DC	PL, PFH_D	ISO 13849-1, IEC 62061 (IEC 61508-2, Anhang C)
	Diagnostic Coverage: Diagnosedeckungsgrad $\Sigma\ \lambda_{DD}/\lambda_{Dtotal}$, mit • λ_{DD}, the rate of detected dangerous hardware failures (die Rate der erkannten Gefahr bringenden Ausfälle) • λ_{Dtotal}, the rate of total dangerous hardware failures (die Rate aller gefahrbringenden Ausfälle)	
Diagnose-Testintervall (T2)	PFH_D, T2	IEC 62061
	Diagnose Testintervall (z. B. alle 8 Stunden wird ein NOT-HALT möglicherweise gedrückt). IEC 62061: siehe z. B. "Anforderungen zum Verhalten (des SRECS) bei Erkennung eines Fehlers im SRECS" (Sicherheitsbezogenes elektrisches Steuerungssystem).	
Diskrepanzzeit Diskrepanzzeit-Überwachung	Gleichzeitigkeit, Synchronisationszeit	
	Die Diskrepanzzeit-Überwachung toleriert durch ein definiertes Zeitfenster die Ungleichzeitigkeit zusammengehöriger Signale.	
Diversität	Redundanz	IEC 60204-1, IEC 61508
	Bei redundanten Anforderungen mit hoher Zuverlässigkeit bei der Erfüllung der Sicherheitsaufgabe sollten die Pfade in unterschiedlichen Konfigurationen konzipiert werden (z. B. eine Drehzahlüberwachung durch Tachogenerator und Fliehkraftschalter): d.h. ungleichartige Mittel zur Ausführung einer geforderten Funktion.	
Drehzahlüberwachung	sichere reduzierte Geschwindigkeit	
	Überwachung der Drehzahl einer mechanischen Bewegung (z. B. Antrieb) in einem definierten Geschwindigkeitsfenster. Diese kann sensorlos (Strom, Frequenz) oder mittels Geber (in der Regel inkremental) erfolgen.	

E

Begriff	Referenz	relevante Norm
E/E/PE	Funktionale Sicherheit	IEC 61508
	electrical and/or electronic and/or programmable electronic technologies of safety related systems: elektrisch/elektronische/programmierbare elektronische Systeme	
Einfehlertoleranz, Einfehlersicherheit	Fehlertoleranz	
	Nach Auftreten eines Fehlers ist die geforderte sichere Funktion weiterhin gewährleistet (z. B. ab der Kategorie 3 nach ISO 13849-1, d. h. ein Fehler führt nicht zum Verlust der Sicherheitsfunktion.	
Einschaltzeit	Sicherheitsschaltgerät	
	Die Zeit vom Anlegen des Steuerkommandos (z. B. NOT–HALT, Positionsschalter, EIN-Taster) bis zum Schließen der Freigabekreise.	
Einschaltzyklus	Selbstüberwachung	
	Automatische zyklische Überwachung der Funktionsfähigkeit der Bauteile durch zyklische Testung.	
Eintrittszeit für Mehrfachfehler (MEZ)	Anforderungsklasse	(nicht mehr gültig) DIN 19250
	Ist die Zeitspanne, in der die Wahrscheinlichkeit für das Auftreten von in Kombination sicherheitskritischen Mehrfachfehlern für die betrachtete Anforderungsklasse hinreichend gering ist. Die Zeitspanne beginnt mit dem letzten Zeitpunkt, an dem sich das betrachtete System in einem nach der betrachteten Anforderungsklasse als fehlerfrei angenommenen Zustand befunden hat.	

Begriff	Referenz	relevante Norm
Erdschlusserkennung	**Querschluss, Kurzschluss** **kurz- und erdschlusssicher Verlegen**	**IEC 60204-1** **DIN VDE 0100, Teil 25**
	Eine Erkennung von Erdschlüssen sofort oder im Rahmen einer zyklischen Selbstüberwachung, wobei das Gerät nach Erkennung des Fehlers einen sicheren Zustand einnimmt.	
Erstfehlereintrittszeit (EEZ)	**Anforderungsklasse**	
	Ist die Zeitspanne, in der die Wahrscheinlichkeit für das Auftreten eines sicherheitskritischen Erstfehlers für die betrachtete Anforderungsklasse hinreichend gering ist. Fehlerbeherrschende Maßnahmen bleiben dabei unberücksichtigt. Die Zeitspanne beginnt mit dem letzten Zeitpunkt, an dem sich das betrachtete System in einem nach der betrachteten Anforderungsklasse als fehlerfrei angenommenen Zustand befunden hat.	
Erweiterungsgerät	**Grundgerät, Sicherheitsschaltgerät**	
	Ein Erweiterungsgerät ist ein Sicherheitsschaltgerät, welches nur in Verbindung mit einem Grundgerät (Basisgerät) zum Zwecke der Kontaktvervielfachung einsetzbar ist.	
ESPE	**BWS, OSSD**	**IEC 61496-1**
	Electro-Sensitive Protective Equipment: berührungslos wirkende Schutzeinrichtung.	

F

Begriff	Referenz	relevante Norm
Federkraftverriegelt	**Positionsschalter, Zuhaltung**	**ISO 12100-1**
	Die Verriegelung erfolgt mit dem Ruhestromprinzip (die Feder verriegelt, der Magnet entriegelt).	
Fehlerausschluss	**FMEA**	**ISO 13849-1** **ISO 13849-2**
	Die Fähigkeit Fehlern zu widerstehen. In einigen Bauteilen können bestimmte Fehler für die Einsatzdauer der SRP/CS ausgeschlossen werden. Z. B. durch sicheres Verlegen kann ein Kurzschluss ausgeschlossen werden. Die Begründung eines Fehlerausschluss muss dokumentiert werden!	
Fehlertoleranz (Hardware-Fehlertoleranz)	**Einfehlertoleranz, Kategorie, Nullfehlertoleranz, SIL, SRECS, SRP/CS**	**IEC 62061**
	Fähigkeit eines SRECS ("sicherheitsbezogenes elektrisches Steuerungssystem"), eines Teilsystems oder Teilsystem-Elements, eine geforderte Funktion beim Vorhandensein von Fehlern oder Ausfällen weiter auszuführen (Widerstandsfähigkeit gegenüber von Fehlern).	
Fehlertoleranzzeit	**Fehlertoleranz**	
	Eigenschaft des Prozesses, die die Zeitspanne beschreibt, in der der Prozess durch fehlerhafte Steuersignale beaufschlagt werden kann, ohne dass ein gefährlicher Zustand eintritt.	
Fehlerreaktionszeiten		
	Benötigte Zeit bis zur Reaktion auf einen aufgedeckten Fehler.	
FMEA	**Fehlerausschluss**	**IEC 60812**
	Failure **M**ode **E**ffect **A**nalysis: Ausfallart und Effektanalyse (Fehlerwirkungsanalyse, Ausfalleffektanalyse). Eine analytische Methode zur systematischen und vollständigen Erfassung potenzieller Fehler und Ausfallzuständen von Komponenten eines Systems sowie deren Auswirkung.	

Begriff	Referenz	relevante Norm
Freigabekreis Freigabestrompfad	**Sicherheitsschaltgerät**	
	Ein Freigabekreis dient der Erzeugung eines sicherheitsgerichteten Ausgangssignals. Freigabekreise wirken nach außen wie Schließer (funktional aber wird immer das sichere Öffnen betrachtet). Ein einzelner Freigabekreis, der intern im Sicherheitsschaltgerät redundant (zweikanalig) aufgebaut ist, kann für Kategorie 3/4 nach ISO 13849-1 eingesetzt werden. *Anmerkung:* *Freigabestrompfade können auch für Meldezwecke (also nicht sicherheitsgerichtet) eingesetzt werden.*	
FTA	**FMEA, Fehlerausschluss**	**IEC 60812**
	Fault Tree Analysis: Fehlerbaumanalyse (FBA). Diese Analyse dient der Ursachenermittlung von Systemversagen, mittels einer deduktiven Top-Down Methode.	
Funktionale Sicherheit	**SRECS**	**IEC 62061, IEC 61508**
	Teil der Gesamtsicherheit, bezogen auf die Maschine und das Maschinen-Steuerungssystem, die von der korrekten Funktion des SRECS ("sicherheitsbezogenes elektrisches Steuerungssystem"), sicherheitsbezogenen Systemen anderer Technologie und externen Einrichtungen zur Risikominderung abhängt (abgeleitet aus IEC 61508-4). *Anmerkung: Funktionale Sicherheit umfasst alle Aspekte, bei denen die Sicherheit von der korrekten Funktion des SRECS, sicherheitsbezogenen Systemen anderer Technologie und externen Einrichtungen zur Risikominderung abhängt.*	
Funktionsblock (FB)	**SRCF**	**IEC 62061**
	Kleinstes Element einer SRCF ("sicherheitsbezogene Steuerungsfunktion"), dessen Ausfall zu einem Ausfall der SRCF führen kann.	
Funktionsprüfung		**IEC 60204-1**
	Die Funktionsprüfung kann entweder automatisch durch das Steuerungssystem oder von Hand durch Überwachung oder Prüfung beim Ablauf und nach festgelegten Zeitabständen oder als Kombination, je nach Erfordernis, ausgeführt werden.	

G

Begriff	Referenz	relevante Norm
Gefahr bringender Ausfall	Ausfall	ISO 12100-1
	(engl. "dangerous failure") Jede Fehlfunktion in der Maschine oder in deren Energieversorgung, die das Risiko erhöht.	
Gefahrenbewertung	Gefährdung, Risikobeurteilung, MRL	ISO 14121 ISO 12100-1
	Die Bewertung einer Gefahr (resultierend aus einer Gefährdung) für den Anwender.	
Gefährdung	Gefahrenbewertung, Risikobeurteilung, MRL	ISO 14121 ISO 12100-1
	Die Gefährdung (durch ein Ereignis) stellt eine Gefahr für den Anwender dar und kann zu einer Verletzung führen (potenzielle Schadensquelle).	
Getrennter Betätiger	Positionsschalter, Zuhaltung	
	Kodiertes, mechanisches Betätigungselement, das bei Herausziehen aus dem Positionsschalter(kopf) die zwangsöffnenden Kontakte öffnet.	
Gleichzeitigkeit Gleichzeitigkeits-Überwachung	Diskrepanzzeit, Zweihandschaltung	EN 547
	Die Gleichzeitigkeits-Überwachung von Signalgebern durch das Sicherheitsschaltgerät wird zur Erhöhung der Funktionalen Sicherheit der Schutzeinrichtung angewendet. Die Überwachung erfolgt indem der Signalwechsel der Signalgeber innerhalb der vorgegeben Zeit, der Synchron-Überwachungszeit, überprüft wird. Wird diese Zeit überschritten, erfolgt kein Freigabesignal. Für einige Sicherheitseinrichtungen ist eine Gleichzeitigkeits-Überwachung vorgeschrieben.	
Grundgerät	Erweiterungsgerät, Sicherheitsschaltgerät	ISO 13849-1
	Ist ein Sicherheitsschaltgerät, das alle Funktionen enthält, die in der jeweiligen Sicherheitseinrichtung vorhanden sein müssen.	

H

Begriff	Referenz	relevante Norm
Handlungen im Notfall	Ausschalten im Notfall, Stillsetzen im Notfall, Notfall Stopp-Funktion, NOT-HALT	IEC 60204-1, Anhang D (Handlungen im Notfall), ISO 12100-1, ISO 13850
	Siehe Ausschalten und Stillsetzen im Notfall: sämtliche Tätigkeiten und Funktionen im Notfall, die auf dessen Beendigung oder Behebung ausgerichtet sind.	
Harmonisierte Norm	MRL, A-B-C - Norm	ISO 12100-1
	Die Typ A (Grundnormen), Typ B (Gruppennormen) und Typ C (Produktnormen) erlauben die Vermutungswirkung (das "Erfüllen" der Maschinenrichtlinie).	

K

Begriff	Referenz	relevante Norm
Kategorien (nach ISO 13849-1)	harmonisierte Norm (B − Norm) Risikoanalyse, Risikobeurteilung	ISO 13849-1

Die Kategorien der ISO 13849-1:2006 (EN 954-1) (B, 1, 2, 3 und 4) erlauben eine Beurteilung der Leistungsfähigkeit sicherheitsbezogener Teile einer Steuerung bei Auftreten von Fehlern.

Kategorie B:
Die Steuerung muss so konzipiert sein, dass sie den zu erwartenden Einflüssen standhalten kann.
Systemverhalten: Ein Fehler kann zum Verlust der Sicherheitsfunktion führen.

Kategorie 1:
Anforderung von B muss erfüllt sein; Verwendung von sicherheitstechnisch bewährten Bauteilen und Prinzipien.
Systemverhalten: Wie Systemverhalten von B, doch mit höherer sicherheitsbezogener Zuverlässigkeit.

Kategorie 2:
Anforderung von B muss erfüllt sein; zusätzliche Prüfung der Sicherheitsfunktion in geeigneten Zeitabständen.
Systemverhalten: Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion zwischen den Prüfabständen führen.

Kategorie 3:
Anforderung von B muss erfüllt sein, ein einzelner Fehler darf nicht zum Verlust der Sicherheitsfunktion führen; einzelne Fehler müssen aufgedeckt werden.
Systemverhalten: Die Sicherheitsfunktion bleibt beim Auftreten einzelner Fehler immer erhalten.

Kategorie 4:
Anforderung von B muss erfüllt sein; der einzelne Fehler muss vor oder bei der nächsten Anforderung der Sicherheitsfunktion erkannt werden.
Systemverhalten: Wenn Fehler auftreten bleibt die Sicherheitsfunktion immer erhalten; die Fehler werden rechtzeitig erkannt.

Reihenschaltung von Sensoren bei Kategorie 3

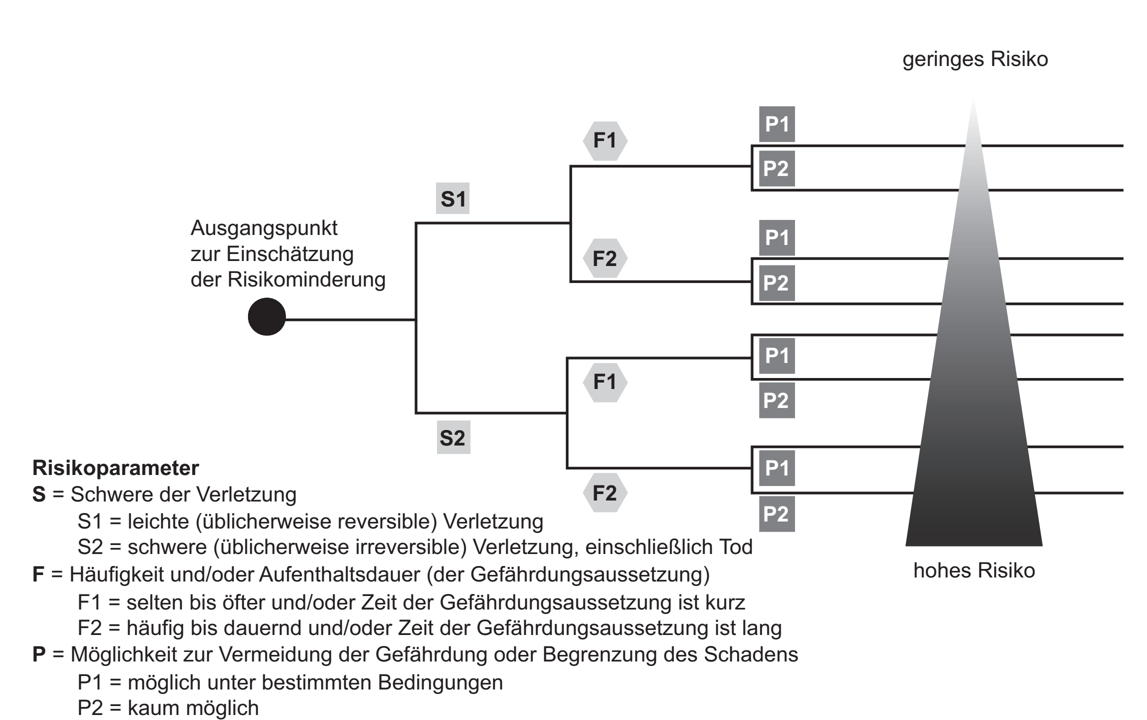
- NOT-HALT: Dürfen immer in Reihe geschaltet werden: das Versagen und gleichzeitige Drücken der Befehlsgeräte kann ausgeschlossen werden.
- Schutztürüberwachung: Positionsschalter dürfen in Reihe geschaltet werden, wenn nicht mehrere Schutztüren gleichzeitig und regelmäßig geöffnet werden (da sonst keine Fehleraufdeckung erfolgen kann).

Reihenschaltung von Sensoren bei Kategorie 4

- NOT-HALT: Dürfen immer in Reihe geschaltet werden: das Versagen und gleichzeitige Drücken der Befehlsgeräte kann ausgeschlossen werden.
- Schutztürüberwachung: Positionsschalter dürfen nie in Reihe geschaltet werden, weil immer jeder gefährliche Fehler aufgedeckt werden muss (unabhängig vom Bedienpersonal).



Begriff	Referenz	relevante Norm
	Risikograf nach ISO 13849-1	



Risikoparameter

S = Schwere der Verletzung
- S1 = leichte (üblicherweise reversible) Verletzung
- S2 = schwere (üblicherweise irreversible) Verletzung, einschließlich Tod

F = Häufigkeit und/oder Aufenthaltsdauer (der Gefährdungsaussetzung)
- F1 = selten bis öfter und/oder Zeit der Gefährdungsaussetzung ist kurz
- F2 = häufig bis dauernd und/oder Zeit der Gefährdungsaussetzung ist lang

P = Möglichkeit zur Vermeidung der Gefährdung oder Begrenzung des Schadens
- P1 = möglich unter bestimmten Bedingungen
- P2 = kaum möglich

a, b, c, d, e = Ziele des sicherheitsgerichteten Performance Level

Begriff	Referenz	relevante Norm
Kaskadiereingang	Sicherheitsschaltgerät sichere Verlegung	
	Sicherer einkanaliger Eingang eines Sicherheitsschaltgerätes, der intern wie ein Sensorsignal ausgewertet wird: logische UND-Verknüpfung mit den anderen Signalgebereingängen: Wenn keine Spannung anliegt, schaltet das Sicherheitsschaltgerät die Freigabekreise (Ausgänge) sicherheitsgerichtet ab. *Anmerkung: durch einen Fehlerausschluss (Kurzschluss) im Schaltschrank kann Kategorie 4 nach ISO 13849-1:2006 (EN 954-1) erreicht werden; durch eine sichere Verlegung kann dieser Fehler ebenfalls außerhalb des Schaltschranks ausgeschlossen werden.*	
Kennzeichnung	MRL, CE, Konformitätserklärung	MRL, (EN 45014)
	Bescheinigung des Maschinenherstellers, dass die Maschine alle relevanten Vorschriften der Maschinenrichtlinie erfüllt, und somit in Verkehr gebracht werden darf. Mit der CE − Kennzeichnung wird dies dem Anwender gezeigt.	
Konformitätserklärung	CE, MRL, Kennzeichnung	MRL, (EN 45014)
	Bescheinigung des Maschinenherstellers, dass die Maschine alle relevanten Vorschriften der Maschinenrichtlinie erfüllt und somit in Verkehr gebracht werden darf. Mit der CE-Kennzeichnung wird dies dem Anwender gezeigt.	
Kurzschluss	Querschluss, Testung	
	Eine nahezu widerstandslose leitende Verbindung zwischen zwei unter Spannung stehenden elektrischen Leitern.	

L

Begriff	Referenz	relevante Norm
Lambda λ	PFH, PFH_D B10, MTTF	IEC 62061
	Rate of failure: Ausfallrate bei ungefährlichen (λ_S) und Gefahr bringenden (λ_D) Fehlern.	
Laserscanner	BWS, AOPD, OSSD	IEC 61496-1
	Ein Sicherheits-Laserscanner dient im stationären wie auch im mobilen Einsatzbereich dem Personenschutz an Maschinen, Robotern, Förderanlagen, Fahrzeugen. Dieser ist ein optischer Flächenscanner und arbeitet berührungslos mit periodisch ausgesendeten Lichtimpulsen, die ein integrierter Drehspiegel in den Arbeitsbereich streut. Dabei werden Personen oder Objekte, die in das definierte Schutzfeld eindringen durch Reflexion dieser Lichtimpulse erkannt. Aus der Lichtlaufzeit werden die Koordinaten des "Hindernisses" errechnet. Die zu überwachende Fläche kann über einen PC innerhalb bestimmter Grenzen frei definiert werden. Befindet sich das "Hindernis" im definierten Schutzfeld, schaltet der Scanner seine sicherheitsgerichteten Ausgänge ab und löst damit eine sicherheitsgerichtete Stopp-Funktion aus.	
Lichtgitter, Lichtvorhang	BWS, AOPD, OSSD	IEC 61496-1
	Ändert bei Unterbrechung eines oder mehrerer Lichtstrahlen ihren Schaltzustand.	
Lichtschranke	BWS, AOPD, OSSD	IEC 61496-1
	Ändert bei Unterbrechung ihres Lichtstrahls ihren Schaltzustand.	
Life time	PFH_D, T1	IEC 62061
	Die Lebenserwartungszeit [h] einer Komponente, die für eine Sicherheitsfunktion erwartet wird.	

M

Begriff	Referenz	relevante Norm
Magnetkraftverriegelt	Positionsschalter, Zuhaltung	ISO 12100-1
	Die Verriegelung erfolgt mit dem Arbeitsstromprinzip (der Magnet verriegelt, die Feder entriegelt).	
Magnetschalter	BWP, Reedkontakte	
	Besteht aus einer kodierten Anordnung mehrerer Reedkontakte, die unter dem Einfluss des zugehörigen Magnetfelds ihren Schaltzustand ändern. Durch die Kodierung ist eine Manipulation ausgeschlossen.	
Manuelle Rückstellung	Start, Wiederanlaufsperre	ISO 13849-1, IEC 60204-1
	Eine Funktion zum Wiederherstellen einer oder mehrer Sicherheitsfunktionen vor einem Neustart der Maschine: Nach der Einleitung eines Stoppbefehls durch eine Schutzeinrichtung muss der Stoppzustand aufrecht erhalten bleiben, bis eine manuelle Rückstelleinrichtung betätigt wird und der sichere Zustand für einen Wiederanlauf gegeben ist.	
Manueller Start	Start, Manuelle Rückstellung	ISO 13849-1, IEC 60204-1
	Das Wiederherstellen der Sicherheitsfunktion erfolgt durch die Überwachung eines statischen Signals, z. B. mit einem Ein-Taster. Ein manueller Start ist nur bis Kategorie 3 nach ISO 13849-1 zulässig, da kein Manipulationsschutz gegeben ist. Diese Startart ist nur zulässig nach erfolgter Gefahrenbeurteilung. *Anmerkung: Mit den Sicherheitsschaltgeräten 3TK28 mit Autostart kann ein manueller Start realisiert werden.*	

<table>
<tr><th>Begriff</th><th>Referenz</th><th>relevante Norm</th></tr>
<tr><td>Maschinensteuerung</td><td>Kategorien
SRP/CS</td><td>ISO 13849-1</td></tr>
<tr><td></td><td colspan="2">Teil der Steuerung (Automatisierung) , der nicht zwangsläufig sicherheitsgerichtet arbeitet, sondern z. B. eine Meldung im Fehlerfall erzeugt.</td></tr>
<tr><td>Maschine</td><td>MRL</td><td></td></tr>
<tr><td></td><td colspan="2">Die Maschine, mit beweglichen Teilen, stellt eine mögliche Gefahr (Gefährdung) für den Anwender dar.
Anmerkung:
Eine Maschine (nach der Maschinenrichtlinie) ist:
• eine Gesamtheit von miteinander verbundenen Teilen oder Vorrichtungen, von denen mindestens eines beweglich ist, sowie gegebenenfalls von Betätigungsgeräten, Steuer- und Energiekreisen usw., die für eine bestimmte Anwendung, wie die Verarbeitung, die Behandlung, die Fortbewegung und die Aufbereitung eines Werkstoffes zusammengefügt sind.
• eine Gesamtheit von Maschinen, die, damit sie zusammenwirken, so angeordnet sind und betätigt werden, dass sie als Gesamtheit funktionieren.
• eine auswechselbare Ausrüstung zur Änderung der Funktion einer Maschine, die nach dem in Verkehr bringen vom Bedienungspersonal selbst an einer Maschine oder einer Reihe verschiedener Maschinen bzw. an einer Zugmaschine anzubringen sind, sofern diese Ausrüstungen keine Ersatzteile oder Werkzeuge sind.</td></tr>
<tr><td>Maschinenrichtlinie</td><td>Maschine, Harmonisierte Norm</td><td></td></tr>
<tr><td></td><td colspan="2">RICHTLINIE 2006/42/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 17. Mai 2006 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten für Maschinen.</td></tr>
<tr><td>Mehrfehlertoleranz,
Mehrfehlersicherheit</td><td>Fehlertoleranz</td><td></td></tr>
<tr><td></td><td colspan="2">Nach Auftreten mehrerer Fehler ist die geforderte sichere Funktion weiterhin gewährleistet.</td></tr>
<tr><td>Meldekreis
Meldestrompfad</td><td>Sicherheitsschaltgerät</td><td></td></tr>
<tr><td></td><td colspan="2">Ein Meldestrompfad dient der Erzeugung eines nicht sicherheitsgerichteten Ausgangssignals. Meldestrompfade können als Öffner oder Schließer realisiert werden.</td></tr>
<tr><td>Mindestbetätigungszeit</td><td>Sicherheitsschaltgerät</td><td></td></tr>
<tr><td></td><td colspan="2">Die kürzeste notwendige Zeit für das Steuerkommando, um das Gerät starten zu können (wiedereinschalten).</td></tr>
<tr><td>MRL</td><td>Maschinenrichtlinie,
Maschine, Harmonisierte Norm</td><td></td></tr>
<tr><td></td><td colspan="2">Maschinenrichtlinie</td></tr>
<tr><td>MTBF</td><td>MTTF, MTTR</td><td>ISO 13849-1</td></tr>
<tr><td></td><td colspan="2">Mean Time Between Failure : Mittlere Ausfallzeit eines Gerätes.
Ist die Summe von MTTF (mean time to failure) und MTTR (mean time to repair).
Es handelt sich bei der mittleren Ausfallzeit um die Zeit, die im normalen Betrieb eines Gerätes oder einer Einrichtung vergeht, bevor ein neuer Fehler auftritt.</td></tr>
<tr><td>MTTF/$MTTF_d$</td><td>MTBF, MTTR, PL</td><td>ISO 13849-1</td></tr>
<tr><td></td><td colspan="2">Mean Time To Failure/Mean Time To Dangerous Failure: Zeit bis zu einem Ausfall bzw. gefährlichen Ausfall.
Die MTTF kann für Bauelemente durch die Analyse von Felddaten oder mittels Vorhersagen durchgeführt werden. Bei einer konstanten Ausfallrate ist der Mittelwert der ausfallfreien Arbeitszeit MTTF = 1/λ , wobei λ die Ausfallrate des Gerätes ist (statistisch gesehen kann angenommen werden, dass nach Ablauf der MTTF 63,2 % der betreffenden Komponenten ausgefallen sind).</td></tr>
</table>

Begriff	Referenz	relevante Norm
MTTR	MTBF, MTTF	ISO 13849-1
	Mean Time To Repair: die mittlere Reparaturzeit eines Gerätes. Die MTTR ist immer bedeutend kleiner als die MTTF.	
Muting	BWS	IEC 61496-1, ISO 13849-1
	Überbrückungsfunktion: Ein zeitlich begrenztes bestimmungsgemäßes Aufheben der Sicherheitsfunktion mit zusätzlicher Sensorik. (ISO 13849-1: vorübergehende automatische Überbrückung einer Sicherheitsfunktion) *Anmerkung: Dies dient in der Praxis der Unterscheidung von Personen und Gegenständen.*	
Muting-Sensoren	Muting, BWS	IEC 61496-1
	Signalgeber, die für einen Muting-Betrieb eingesetzt werden, um einen Körper zu erkennen, bei denen eine BWS nicht abschalten soll.	

N

Begriff	Referenz	relevante Norm
Näherungsschalter		
	(induktiv, kapazitiv oder optisch) Ist ein Schaltelement, welches bei der Annäherung von Körpern oder Flüssigkeiten seinen Schaltzustand ändert (je nach Ausführung). Näherungsschalter sind überwiegend mit Halbleiterausgängen ausgerüstet.	
Netzausfall Überbrückung	Sicherheitsschaltgerät, BWS	
	Maximale Zeit für Kurzzeitunterbrechungen der Versorgungsspannung, welche nicht zu einer Fehlfunktion oder zum Rücksetzen des Gerätes führt.	
NFPA79 (USA)	NRTL, OSHA	
	Electrical Standard for industrial Machinery in den USA: Dieser Standard gilt für die elektrische Ausrüstung von Industriemaschinen mit Nennspannungen kleiner 600V. Die Neufassung NFPA 79-2002 enthält grundlegende Anforderungen für programmierbare Elektronik und Busse, wenn diese zur Ausführung sicherheitsrelevanter Funktionen eingesetzt werden. Bei Erfüllung dieser Anforderungen dürfen elektronische Steuerungen und Busse auch für NOT-HALT Funktionen der Stopp-Kategorien 0 und 1 verwendet werden (siehe NFPA 79-2002 9.2.5.4.1.4). Im Unterschied zu EN 60204-1 verlangt NFPA 79 bei NOT-HALT Funktionen die elektrische Energie durch elektromechanische Mittel abzutrennen.	
Notfall	Ausschalten im Notfall Stillsetzen im Notfall Handlungen im Notfall	IEC 60204-1, Anhang D (Handlungen im Notfall) ISO 12100-1
	Eine Gefährdungssituation, die dringend beendet werden muss oder dringender Abhilfe bedarf. Ein Notfall kann entstehen: • beim normalen Betrieb der Maschine (z. B. durch menschlichen Eingriff oder als Folge äußerer Einflüsse) • als Folge einer Fehlfunktion oder des Ausfalls irgendeines Teils der Maschine	
NOT-AUS ("emergency switching off")	Ausschalten im Notfall NOT-HALT	ISO 13850 IEC 60204-1 Anhang D
	Eine Handlung im Notfall, die dazu bestimmt ist, die Versorgung mit elektrischer Energie zu einer ganzen oder zu einem Teil einer Installation abzuschalten, falls ein Risiko für elektrischen Schlag oder ein anderes Risiko elektrischen Ursprungs besteht: Die Gefahr soll schnellstmöglich beendet werden, z. B. durch einen "Trenner" in einer Haupteinspeisung.	

Begriff	Referenz	relevante Norm
NOT-HALT ("emergency stop")	Stillsetzen im Notfall NOT-AUS	ISO 13850 IEC 60204-1 Anhang D
	Eine Handlung im Notfall, die dazu bestimmt ist, einen Prozess oder eine Bewegung anzuhalten, der (die) Gefahr bringen würde (Stillsetzen). *Anmerkung: Durch eine einzige Handlung einer Person wird die Funktion NOT-HALT ausgelöst. Diese muss nach ISO 13849-1 zu jeder Zeit verfügbar und funktionsfähig sein. Die Betriebsart bleibt dabei unberücksichtigt.*	
NOT-HALT Befehlsgerät	Pilzdrucktaster, NOT-HALT, Seilzugschalter, Zwangsöffnung	ISO 13850 IEC 60204-1
	Schaltelement, welches in Gefahrensituationen betätigt, ein Stillsetzen des Prozesses oder der Maschine bzw. Anlage bewirkt. Dieser muss über zwangsöffnende Kontakte verfügen und sollte leicht erreichbar und überlistungssicher sein.	
NOT-HALT Einrichtung	NOT-HALT	ISO 13850, IEC 60204-1
	Eine NOT-HALT Einrichtung ist eine Schutzeinrichtung für die Handlung im Notfall.	
NRGF NIPF NIPM	NRTL, NFPA79	
	"Kategorien" bei UL 508 (die Basisnorm für die NRTL-Listung): NRGF: Programmable Safety Controllers NIPF: Active Opto-electronic Protective Devices NIPM: Active Opto-electronic Protective Devices Responsive to Diffuse Reflection	
NRTL	NFPA79, OSHA, NRGF, NIPF, NIPM	
	Nationally **R**ecognized **T**esting **L**aboratory: hier können Produkte gelistet werden, damit diese in den USA zweckgemäß (nach der NFPA79) verwendet werden dürfen. Eine NRTL-Listung entspricht einer Zertifizierung. Anwendung für Safety Produkte: Die Anforderung "listed for such use" ist wie folgt zu verstehen. Die Basisnorm für die Listung ist UL 508. Ein NRTL (z. B. UL) bestätigt durch Eintrag in eine "Liste", dass das betreffende Gerät die Anforderungen von UL 508 erfüllt.	
NSR		IEC 60439-1, IEC 60204-1
	Nieder**s**pannungs**r**ichtlinie in Europa (73/23/EWG) (für den Schaltschrankbau in der IEC 60439-1 umgesetzt). Die IEC 60204-1 ist unter der NSR gelistet.	
Nullfehlertoleranz	Fehlertoleranz	
	Nach Auftreten eines Fehlers ist die geforderte sichere Funktion nicht mehr gewährleistet.	

O

Begriff	Referenz	relevante Norm
OSHA	NRTL	
	Occupational Safety and Health Act (www.osha.gov) Ein wesentlicher Unterschied bei den gesetzlichen Anforderungen zur Sicherheit am Arbeitsplatz zwischen USA und Europa ist, dass es in den Vereinigten Staaten keine einheitliche Bundesgesetzgebung zur Maschinensicherheit gibt, welche die Verantwortlichkeit des Herstellers/Lieferers abdeckt. Vielmehr besteht die generelle Anforderung, dass der Arbeitgeber einen sicheren Arbeitsplatz bieten muss. Die OSHA Regeln unter 29 CFR 1910 enthalten allgemeine Anforderungen für Maschinen (1910.121) und eine Reihe spezifischer Anforderungen für bestimmte Maschinentypen. Die Anforderungen darin sind sehr spezifisch aber technisch wenig detailliert. Neben den OSHA Regeln ist es wichtig, die aktuellen Standards von Organisationen wie NFPA und ANSI sowie die in USA bestehende umfassende Produkthaftung zu beachten.	
OSSD	BWS, ESPE	IEC 61496-1
	Output Signal Switching Device, Ausgangsschaltelement – Der Teil der BWS, der in den AUS-Zustand übergeht, wenn die Sicherheitslichtschranke, -lichtvorhang, -lichtgitter oder die Überwachungseinrichtungen ansprechen.	

P

Begriff	Referenz	relevante Norm
parts count Verfahren	Lambda λ, MTTF	IEC 61709
	DIN EN 61709 "Bauelemente der Elektronik – Zuverlässigkeit – Referenzbedingungen für Ausfallraten und Beanspruchungsmodelle zur Umrechnung (IEC 61709:1996); Deutsche Fassung EN 61709:1998" (EN/IEC 61709 "Electronic components – Reliability – Reference conditions for failure rates in stress models for conversion:1996") beschreibt eine Methode sowie Umrechnungsmodelle zum Berechnen von Ausfallraten, beinhaltet jedoch keine eigenen Ausfallratenwerte.	
PL Performance Level		ISO 13849-1
	Fähigkeit von sicherheitsbezogenen Teilen, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen (die in Betracht gezogen werden sollten), um die erwartete Risikominderung zu erfüllen: von PL a (höchste Ausfallwahrscheinlichkeit) bis PL e (niedrigste Ausfallwahrscheinlichkeit). Darüber hinaus bietet die Siemens Werksnorm SN 29500 neben oben genannten Methoden und Modellen auch Standard-Ausfallratenwerte für elektronische und elektromechanische Komponenten.	
PDF PFD		IEC 61508, IEC 62061
	Probability of dangerous failure: Wahrscheinlichkeit Gefahr bringender Ausfälle. Probability of failure on demand: Ausfallwahrscheinlichkeit bei Auslösen/Anfrage der Sicherheitsfunktion.	
PFH PFH_D	B10, C, CCF, Lambda λ	IEC 62061
	Probability of failure per hour: Ausfallwahrscheinlichkeit pro Stunde, zur Ermittlung der "random integrity". Probability of dangerous failure per hour: Wahrscheinlichkeit Gefahr bringender Ausfälle pro Stunde.	

Begriff	Referenz	relevante Norm
Pilztaster (Pilzdrucktaster)	**NOT-HALT Befehlsgeräte**	**ISO 13850, IEC 60204-1**
	NOT-HALT Befehlsgerät, das die Form eines Pilzes aufweist.	
Prellzeit	**Positionsschalter**	
	Zeitdauer vom ersten bis zum letzten Schließen bzw. Öffnen eines Kontaktes (bei Standardschalter mit Sprungkontakten ca. 2 bis 4 ms).	
Proof test **Proof test interval**	**PFH_D, T1**	**IEC 62061**
	Proof test: Wiederholungsprüfung, wiederkehrende Prüfung, die zur Erkennung von Fehlern in einem SRECS ausgeführt wird, sodass, falls notwendig, das System in einen "Wie-Neu-Zustand" gebracht oder so nah wie praktisch möglich an diesen Zustand heran gebracht werden kann (abgeleitet aus der IEC 61508-4).	
PROFIsafe	**ASIsafe**	
	Sicherheitsgerichtete Kommunikation über den Standard PROFIBUS (schwarzer Kanal).	
Positionsschalter	**Standard-Positionsschalter, Zuhaltung, getrennter Betätiger, Zwangsöffnung**	**EN 50041, EN 50047**
	Teil der Verriegelungseinrichtung einer trennenden Schutzeinrichtung, der seinen Schaltzustand in Abhängigkeit von einem mechanisch gegebenen Steuerbefehl ändert. Es gibt Positionsschalter mit und ohne Zuhaltung, mit und ohne getrennten Betätiger. *Anmerkung: Überwiegend werden Standard-Positionsschalter gemäß (EN 50047 und EN 50041) eingesetzt.*	

Q

Begriff	Referenz	relevante Norm
Querschluss	**Kategorien, Kurzschluss, Testung**	**ISO 13849-1**
	Kann nur bei mehrkanaliger Geräteansteuerung auftreten und ist ein Schluss zwischen Kanälen (z. B. im zweikanaligen Sensorkreis)	
Querschlusserkennung	**Kategorien (insb. 3/4)** **Testung**	**ISO 13849-1**
	Die Fähigkeit eines Sicherheitsschaltgerätes, Querschlüsse sofort oder im Rahmen einer zyklischen Überwachung zu erkennen: Das Gerät nimmt nach Erkennung des Fehlers einen sicheren Zustand ein.	

R

Begriff	Referenz	relevante Norm
Redundanz		
	Die Anwendung von mehr als einem Gerät oder System soll sicherstellen, dass bei Ausfall von Funktionen eines Gerätes oder Systems ein anderes für diese Funktion verfügbar ist. *Anmerkung: Bei Redundanz (z. B. mehrkanaliger Aufbau) wird die Widerstandsfähigkeit gegenüber von Fehlern erhöht. Dies kann zur Erhöhung der Sicherheit und/oder Verfügbarkeit genutzt werden.*	
Reedkontakt	BWP, Magnetschalter	
	Reedkontakte werden durch einen Magneten geschlossen, und öffnen sich sobald der Magnet wieder weg ist: Sie reagieren also auf ein magnetisches Feld.	
Reihenschaltung	Kategorien	ISO 13849-1
	Sensoren, z. B. NOT-HALT Befehlsgeräte, werden in Reihe geschaltet und mittels eines Sicherheitsschaltgerätes ausgewertet (siehe erreichbare Kategorie Seite 1 bis 6).	
Relais	Sicherheitsschaltgerät	
	Sicherheitsrelais sind intern redundant und mit zwangsgeführten Kontakten ausgeführt (Hersteller z. B. Matsushita, NAIS) und werden als Freigabekreis(e) im Sicherheitsschaltgerät verwendet.	
Reset	Start, Sicherheitsschaltgerät	
	Einschaltfunktion (EIN), die eine Wiederanlaufsperre darstellt.	
Reset-Taster	Start, Sicherheitsschaltgerät	
	Der EIN – Taster stellt in einem Sicherheitsschaltgerät eine Wiederanlaufsperre dar, welche erst durch Betätigung aufgehoben wird.	
Risiko (Risikoelemente)	Risikobeurteilung, Gefahr	ISO 14121 ISO 12100-1
	Die Kombination der Wahrscheinlichkeit eines Schadenseintritts und des Schadensausmaßes.	
Risikoanalyse Risikobeurteilung	Risiko, Gefahr	ISO 14121 ISO 12100-1
	Die Norm ISO 14121 enthält Verfahren, die für die Durchführung einer Risikobeurteilung notwendig sind. Die Risikobeurteilung umfasst demnach zunächst eine Risikoanalyse und eine anschließende Risikobewertung.	
Rückfallzeit	Sicherheitsschaltgerät	
	Die Zeit vom Abschalten des Steuerkommandos oder der Versorgungsspannung bis zum Öffnen der Freigabekreise (Freigabestrompfade).	
Rückführkreis	Sicherheitsschaltgerät	ISO 13849-1
	Dient der Überwachung angesteuerter Aktoren (z. B. Relais oder Lastschütze mit zwangsgeführten Kontakten). Die Auswerteeinheit kann nur bei geschlossenem Rückführkreis aktiviert werden. *Anmerkung: In Reihe geschaltete Öffner (zwangsgeführte Kontakte) der zu überwachenden Lastschütze werden in den Rückführkreis des Sicherheitsschaltgerätes integriert. Verschweißt ein Kontakt im Freigabekreis, so ist ein erneutes Aktivieren des Sicherheitsschaltgerätes nicht mehr möglich, weil der Rückführkreis geöffnet bleibt.* *Die (dynamische) Überwachung des Rückführkreises muss nicht sicher sein, weil diese nur der Fehleraufdeckung dient: Der EIN-Taster wird meistens mit den zwangsgeführten Kontakten der Aktoren in Reihe geschaltet (Fehleraufdeckung bei Start).*	

S

Begriff	Referenz	relevante Norm
Schaltmatten, Schaltleisten, Schaltkanten, Schaltpuffer	**Sicherheitsbauteil**	**EN 1760-1, -2, -3**
	Sind Signalgeber, die bei Betreten (Schaltmatte) bzw. bei Verformung (Schaltleisten, Schaltkanten) ihren Schaltzustand ändern. Schaltmatten erzeugen einen Querschluss bei Betreten.	
Schutztürwächter	**Sicherheitsschaltgerät**	**ISO 13849-1**
	Eine Auswerteeinheit, welche die Stellung von Positionsschaltern an einer trennenden Schutzeinrichtung überwacht. Sie erzeugt ein sicherheitsgerichtetes Ausgangssignal, wenn diese Schutztür geschlossen wird. Herkömmliche Sicherheitsschaltgeräte, wie z. B. die 3TK28, übernehmen diese Funktion heute.	
Seilzugschalter	**Standard-Positionsschalter, Zuhaltung, getrennter Betätiger, Zwangsöffnung**	**EN 50043, EN 50047**
	Wird meist in NOT-HALT Einrichtungen verwendet und ist ein Signalgeber der seinen Schaltzustand ändert, wenn eine an ihm befestigte Reißleine gezogen wird, bzw. das Seil reißt. Dient der Überwachung ausgedehnter Anlagen (z. B. Förderstrecken).	
Selbstüberwachung	**Diagnose-Testintervall, T2**	**IEC 62061**
	Automatische zyklische Überwachung der Funktionsfähigkeit der Bauteile durch zyklische Testung.	
Sensitive Schutzeinrichtung (SPE)		**ISO 12100-1**
	Sensitive protection equipment: mechanisch behaftetes Betriebsmittel (nicht berührungslos).	
SFF	**DC, PFH_D**	**IEC 62061**
	Anteil sicherer Ausfälle Anteil an der Gesamtausfallrate eines Teilsystems, der nicht zu einem Gefahr bringenden Ausfall führt. *Anmerkung: Der Anteil sicherer Ausfälle (SFF) kann nach folgender Gleichung berechnet werden:* $(\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_D)$, *wobei λ_S die Rate ungefährlicher Ausfälle,* *λ_{DD} die Rate Gefahr bringender Ausfälle, die durch die Diagnosefunktionen erkannt werden, und λ_D die Rate Gefahr bringender Ausfälle ist.*	
Sicher reduzierte Geschwindigkeit		**IEC 60204-1, IEC 61800**
	Die Funktion erlaubt die Überwachung einer Achse oder Spindel auf eine vorgegebene Geschwindigkeit. Beim Einrichten sind z. B. die Geschwindigkeitsgrenzen entsprechend der geltenden C-Norm anzuwenden, z. B. 2 m/min für Achsen. In vielen Maschinen kommt eine sicher überwachte Geschwindigkeit aber auch während der automatischen Bearbeitung zur Anwendung. Um Schaden an der Maschine oder am Produktionsgut zu vermeiden, kann so die Überschreitung bestimmter Höchstdrehzahlen und Geschwindigkeiten sicher verhindert werden. Durch den Antriebshersteller müssen Schutzmaßnahmen vorgesehen werden, die das Ändern der Geschwindigkeitsgrenzwerte nur dem Maschinenhersteller erlauben. Nach jeder Neueinstellung oder Änderung von Geschwindigkeitsgrenzwerten muss außerdem ein Abnahmetest durchgeführt werden. Der Inbetriebnehmer muss während des Abnahmetestes den Geschwindigkeitsgrenzwert anfahren und einwandfreie sicherheitsgerichtete Reaktion in einem vom Antriebshersteller vorgesehenen Formblatt dokumentieren. *Anmerkung: Kann auch für das Erkennen von "Übergeschwindigkeit" (overspeed) genutzt werden.*	
Sicherheitsabstand	**BWS**	**EN 999**
	Definiert die notwendigen Abstände und Geschwindigkeiten einer Person, die als Eingangsgröße für eine Gefahrenbetrachtung dienen (z. B. für Lichtvorhänge, Laserscanner, ...).	

<table>
<tr><th>Begriff</th><th>Referenz</th><th>relevante Norm</th></tr>
<tr><td>Sicherer Betriebshalt</td><td>sicheres Stillsetzen</td><td>IEC 60204-1, IEC 61800-5-2</td></tr>
<tr><td></td><td colspan="2">Im Gegensatz zum Sicheren Halt bleiben die Antriebe beim Sicheren Betriebshalt voll in Regelung. Die übergeordnete zweikanalige Sicherheitssteuerung wird permanent mit den Positionswerten versorgt und leitet bei Abweichungen von der Stillstandsposition eine sicherheitsgerichtete Reaktion ein.

Der Sichere Betriebshalt wird immer dort benötigt, wo häufig manuell in den Prozess eingegriffen werden muss, eine hardwaremäßige Trennung von der Energieversorgung aber aus technologischen Gründen nicht praktikabel ist. Anwendungsbeispiele sind der Einrichtbetrieb und das Einfahren von CNC-Programmen.</td></tr>
<tr><td>Sicher abgeschaltetes Moment (Sicherer Halt)</td><td>sicheres Stillsetzen</td><td>IEC 60204-1, IEC 61800-5-2</td></tr>
<tr><td></td><td colspan="2">Beim sicher abgeschalteten Moment ist die Energieversorgung zum Antrieb sicher unterbrochen. Der Antrieb darf kein Drehmoment und somit keine gefährliche Bewegung erzeugen können. Eine Überwachung der Stillstandsfunktion muss nicht erfolgen. Eine kontaktbehaftete Trennung zur Energieversorgung kann, muss jedoch nicht verwendet werden.

Externe Ansteuerung:

Einige Antriebssysteme bieten die Möglichkeit, das sicher abgeschaltete Moment von extern über Klemmen anzusteuern. Hierbei ist anhand der Herstellerunterlagen zu prüfen, ob eine Weiterverarbeitung des Rückmeldekontaktes in der Maschinesteuerung notwendig ist. Das Kleben oder Nichtanziehen kann auch bei einem Sicherheitsrelais nicht ausgeschlossen werden. Erst die sichere Weiterverarbeitung des zwangsgeführten Rückmeldekontaktes ergibt schließlich eine sichere Schaltung. Die achsweise ansteuerbaren Relais überbrücken bei einwandfreier Funktion des Sicheren Halts den Freigabepfad der Relaiskombination für die Schutztüren. Bei Versagen des Relais wird das übergeordnete Netzschütz abgeschaltet.

Interne Ansteuerung:

Wird das sicher abgeschaltete Moment intern angesteuert, z. B. durch das redundante Rechnersystem der Antriebssteuerung, ist bereits durch den Antriebshersteller zu gewährleisten, dass das Relais sicher zurückgelesen wird. Beispiele für eine interne Ansteuerung sind z. B. die Abschaltung nach einer Fehlerreaktion, z. B. nach Überschreitung von Geschwindigkeits- oder Positionsgrenzwerten bzw. bei der Durchführung der Zwangsdynamisierung des Abschaltpfades (Teststopp).</td></tr>
<tr><td>Sichere Trennung
• von Stromkreisen
• von AS-i Modulen</td><td>sicheres Verlegen, Positionsschalter</td><td>IEC 61140
(EN 50178)</td></tr>
<tr><td></td><td colspan="2">Ziel ist die Betriebssicherheit, Schutz der Spannungsverschleppung, bei unterschiedlichen Spannungen in einem Kabel oder Betriebsmittel, das für die höchste Spannung isoliert sein muss

(Schutz gegen elektrischen Schlag):
• Leitungsisolierung zwischen zwei Leitern unterschiedlicher Potenziale;
• AS-i Module müssen zwischen AS-Interface und U_{hilf} die Anforderungen gemäß EN 50187 bzgl. der Luft- und Kriechstrecken und der Spannungsfestigkeit der Isolation der relevanten Bauteile erfüllen.</td></tr>
</table>

<table>
<tr><th>Begriff</th><th>Referenz</th><th>relevante Norm</th></tr>
<tr><td>Sicheres Stillsetzen
Stillsetzen im Notfall</td><td>NOT-HALT</td><td>IEC 61800
IEC 60204-1</td></tr>
<tr><td></td><td colspan="2">Beim sicheren Stillsetzen erfolgt ein der Gefahrensituation entsprechendes Stillsetzen des Antriebs.
Dabei müssen die elektrischen, elektronischen, elektromechanischen Einrichtungen, die für die Verzögerung des Antriebs notwendig sind, in die Sicherheitsbetrachtungen mit einbezogen werden, unter Berücksichtigung weiterer Schutzmaßnahmen.
Geeignet sind z. B.:
• gesteuertes Stillsetzen mit sicher überwachter Verzögerungszeit
• gesteuertes Stillsetzen mit sicherer Überwachung der Bremsrampe
• ungesteuertes Stillsetzen mit mechanischen Bremsen
Anwendungsbeispiele sind z. B.: Zustimmungsschalter, elektrische Verriegelung von beweglichen Schutzeinrichtungen oder Reaktion nach Erkennen von Fehlern.</td></tr>
<tr><td>Sicherheitsbauteil</td><td>MRL</td><td>MRL Anhang IV</td></tr>
<tr><td></td><td colspan="2">Diese sind im Anhang IV der Maschinenrichtlinie gelistet, wie z. B.:
• Sensorgesteuerte Personenschutzeinrichtungen (Lichtschranken, Schaltmatten, elektromagnetische Detektoren)
• Selbsttätige bewegliche Schutzeinrichtungen an Maschinen gemäß Buchstabe A Nummer 9, 10 und 11
• Zweihandschaltungen
• Überrollschutzaufbau
• Schutzaufbau gegen herabfallende Gegenstände
Anmerkung: In der Maschinenrichtlinie Artikel 1, Abs. (2) ist ein Sicherheitsbauteil, soweit es sich nicht um eine auswechselbare Ausrüstung handelt, ein Bauteil, das vom Hersteller oder seinem in der Gemeinschaft niedergelassenen Bevollmächtigten mit dem Verwendungszweck der Gewährleistung einer Sicherheitsfunktion in den Verkehr gebracht wird und dessen Ausfall oder Fehlfunktion die Sicherheit oder die Gesundheit der Personen im Wirkbereich der Maschine gefährdet.</td></tr>
<tr><td>Sicherheitseinrichtung</td><td>Maschine</td><td>MRL</td></tr>
<tr><td></td><td colspan="2">Ist überall da notwendig, wo Gefahren für Mensch, Maschinen und Umwelt auftreten können.</td></tr>
<tr><td>Sicherheitskombination</td><td>Auswerteeinheit, Sicherheitsschaltgerät</td><td></td></tr>
<tr><td></td><td colspan="2">Alter Begriff für Sicherheitsschaltgerät oder Auswerteeinheit.</td></tr>
<tr><td>Sicherheitsschaltgerät</td><td>Auswerteeinheit, SRECS, SRP/CS</td><td></td></tr>
<tr><td></td><td colspan="2">Weiterer Begriff für Sicherheitskombination oder Auswerteeinheit.
Eine sicherheitsgerichtete Auswerteeinheit erzeugt, abhängig vom Zustand angeschlossener Signalgeber, entweder nach einer festen Zuordnung oder nach programmierten/parametrierten Anweisungen ein sicherheitsgerichtetes Ausgangssignal.</td></tr>
<tr><td>Sicheres Verlegen</td><td>Sichere Trennung (von Stromkreisen)</td><td>IEC 61140
(Schutz gegen elektrischen Schlag)</td></tr>
<tr><td></td><td colspan="2">Basisisolierte Leiter nicht auf scharfe Kanten oder z. B. in Stahlrohr verlegen (Schutzklasse 2): dient dem Fehlerausschluss (höchste Isolierung).</td></tr>
</table>

<table>
<tr><th>Begriff</th><th>Referenz</th><th>relevante Norm</th></tr>
<tr><td>SIL, Safety Integrity Level
SIL CL, SIL claim limit
Sicherheits-Integritätslevel</td><td>PFD, PFH_D, SRECS</td><td>IEC 61508
IEC 62061</td></tr>
<tr><td></td><td colspan="2">Eine von drei Möglichkeiten zur Festlegung der Anforderungen zur Sicherheitsintegrität der Sicherheitsfunktionen, die SRECS zugeordnet werden, wobei der Sicherheits-Integritätslevel 3 den höchsten und der Sicherheits-Integritätslevel 1 den niedrigsten Sicherheits-Integritätslevel darstellst.
SIL claim limit (EN 62061):
Der Sicherheits-Integritätslevel, der für das SRECS in Anspruch genommen werden kann, muss geringer oder gleich dem niedrigsten Wert der SIL–Anspruchsgrenzen für die Sicherheitsintegrität der Hardware, der systematischen Integrität und den strukturellen Einschränkungen von irgendeinem der Teilsysteme sein.
Anmerkung: Das Zielmaß zur Bestimmung der Leistungsfähigkeit einer Sicherheitsfunktion (Funktionale Sicherheit), der Begriff wurde in der englischen Fassung der IEC 61508 eingeführt: In der IEC 62061 wird ein SIL (PFH_D) und in der ISO 13849-1 ein PL für eine Ausfallwahrscheinlichkeit ermittelt.</td></tr>
<tr><td>Spiegelkontakt</td><td></td><td></td></tr>
<tr><td>SRCF</td><td>Funktionale Sicherheit, SRECS</td><td>IEC 62061</td></tr>
<tr><td></td><td colspan="2">(engl.: Safety-Related Control Function) Vom SRECS ausgeführte sicherheitsbezogene Steuerungsfunktion mit einem festgelegten Integritätslevel, die dazu vorgesehen ist, den sicheren Zustand der Maschine aufrechtzuerhalten oder einen unmittelbaren Anstieg von Risiken zu verhindern.</td></tr>
<tr><td>SRECS</td><td>Funktionale Sicherheit, SRP/CS, Sicherheitsschaltgerät, Auswerteeinheit</td><td>IEC 62061</td></tr>
<tr><td></td><td colspan="2">(engl.: Safety-Related Electrical Control Systems) Sicherheitsbezogenes elektrisches Steuerungssystem einer Maschine, dessen Ausfall zu einer unmittelbaren Erhöhung von Risiken führt.</td></tr>
<tr><td>SRP/CS</td><td>Maschinensteuerung, Auswerteeinheit, Sicherheitsschaltgerät</td><td>ISO 13849-1</td></tr>
<tr><td></td><td colspan="2">(engl.: Safety-Related Parts of Control Systems) Sicherheitsbezogenes Teil einer Steuerung, das auf sicherheitsbezogene Eingangssignale reagiert und sicherheitsbezogene Ausgangssignale erzeugt.</td></tr>
<tr><td>Start (automatisch, manuell oder überwacht)</td><td>Taster-Überwachung, Manuelle Rückstellung</td><td>ISO 13850, IEC 60204-1, ISO 13849-1</td></tr>
<tr><td></td><td colspan="2">Ein Sicherheitsschaltgerät kann manuell, überwacht oder automatisch gestartet werden. Bei einem manuellen oder überwachten Start wird durch das Betätigen des Ein-Tasters nach Prüfung des Eingangsabbildes und nach positivem Test des Sicherheitsschaltgerätes ein Freigabesignal erzeugt. Diese Funktion wird auch als statischer Betrieb bezeichnet und ist z. B. für Not-Halt-Einrichtungen vorgeschrieben (IEC 60204-1, bewusste Handlung). Der überwachte Start wertet – im Gegensatz zum manuellen Start – einen Signalwechsel des Ein-Tasters aus. Somit kann die Bedienung des Ein-Tasters nicht überlistet werden. Der manuelle Start ist bis Kategorie 3 nach ISO 13849-1 zulässig, jedoch muss der überwachte Start für Kategorie 4 nach ISO 13849-1 eingesetzt werden.
Bei einem automatischen Start wird ohne manuelle Zustimmung, aber nach Prüfung des Eingangsabbildes und positivem Test des Sicherheitsschaltgerätes ein Freigabesignal erzeugt. Diese Funktion wird auch als dynamischer Betrieb bezeichnet und ist für Not-Halt-Einrichtungen unzulässig. Nicht hintertretbare trennende Schutzeinrichtungen können mit dem automatischen Start arbeiten.
Diese Startart ist nur zulässig nach erfolgter Gefahrenbeurteilung.</td></tr>
<tr><td>Standard-Positionsschalter</td><td>Zuhaltung, getrennter Betätiger</td><td>EN 50041, EN 50047</td></tr>
<tr><td></td><td colspan="2">Die Bauformen der Standard-Positionsschalter sind in kleine (EN 50047) und große (EN 50041) Bauformen aufgeteilt.</td></tr>
</table>

Begriff	Referenz	relevante Norm
Stellungsüberwachung	**Positionsschalter**	
	Stellungsüberwachung ist die Überwachung der Position einer Schutzeinrichtung, wie z. B. einer Schutztür, mit Hilfe dafür geeigneter Signalgeber und Sicherheitsschaltgeräte.	
Stillsetzen im Notfall	**Stillsetzen im Notfall, Handlungen im Notfall, Notfall Stopp-Funktion, NOT-HALT**	**IEC 60204-1, Anhang D (Handlungen im Notfall) ISO 12100-1 ISO 13850**
	Eine Handlung im Notfall, die dazu bestimmt ist, einen Prozess oder eine Bewegung anzuhalten, der (die) Gefahren bringen würde. Das Stillsetzen im Notfall muss entweder als eine Stopp-Kategorie 0 oder 1 wirken. Die Stopp-Kategorie für das Stillsetzen im Notfall muss anhand der Risikobeurteilung für die Maschine festgelegt werden.	
Stillstandsüberwachung	**Stopp-Funktion, sichere reduzierte Geschwindigkeit, sicheres Stillsetzen**	**ISO 13850 IEC 60204-1**
	Geberlose oder geberbehaftete Überwachung einer Antriebsfunktion mit einer definierten Drehzahl: Dies entspricht einer Drehzahlüberwachung mit N = 0 U/min.	
Stopp-Funktion	**Ausschalten im Notfall, Stillsetzen im Notfall**	**ISO 13850 IEC 60204-1**
	Stopp Kategorie 0 Ungesteuertes Stillsetzen durch sofortiges Abschalten der Energie zu den Maschinenantriebselementen. **Stopp Kategorie 1** Gesteuertes Stillsetzen bei dem die Energiezufuhr erst dann unterbrochen wird, wenn der Stillstand erreicht ist. **Stopp Kategorie 2** Gesteuertes Stillsetzen bei dem die Energiezufuhr im Stillstand erhalten bleibt.	
Strukturelle Einschränkung	**SIL, SIL CL, Teilsystem**	**IEC 62061**
	Anzahl von strukturellen Anforderungen, die den SIL einschränken, der für ein Teilsystem geltend gemacht werden kann.	
Synchron-Überwachungszeit	**Zweihandschaltung, Diskrepanzzeit**	**EN 574**
	Ist die Zeit, in der eine gleichzeitige Betätigung erfolgen muss, um ein sicheres Ausgangssignal zu erzeugen (in der Regel < 0,5 s).	
Systematische Sicherheitsintegrität	**SIL, SIL CL, SRECS, Teilsystem**	**IEC 61508, IEC 62061**
	Teil der Sicherheitsintegrität eines SRECS oder seiner Teilsysteme in Bezug auf seine/ihre Widerstandsfähigkeit gegenüber systematischen Ausfällen mit Gefahr bringenden Auswirkungen.	

T

Begriff	Referenz	relevante Norm
T1	**PFH_D** **Proof test interval, lifetime**	**IEC 62061**
	Kleinster Wert von Proof test interval (Wiederholungsprüfung) oder lifetime (Lebenserwartungszeit) [h] (z. B. T1 = 10^5 [h] entspricht einer Lebenserwartungszeit von 100.000 Stunden bzw. ca. 11,4 Jahren). *Anmerkung: In der EN 62061 wird dieser Wert für einen vereinfachten Ansatz zur Abschätzung der Wahrscheinlichkeit Gefahr bringender zufälliger Hardwareausfälle von Teilsystemen benötigt.*	
T2	**PFH_D**	**IEC 62061**
	Diagnostic test interval: Diagnose Testintervall IEC 62061: siehe "Anforderungen zum Verhalten (des SRECS) bei Erkennung eines Fehlers im SRECS" (Sicherheitsbezogenes elektrisches Steuerungssystem) *Anmerkung: Die mittlere Zeit bis zur Wiederherstellung, die im Zuverlässigkeitsmodell betrachtet wird, muss das Diagnose-Testintervall, die Reparaturzeit und alle anderen Verzögerungen vor der Wiederherstellung berücksichtigen.*	
Taster-Überwachung	**Start, überwachter Start** **Kategorien**	**ISO 13849-1**
	Die Funktion des Tasters (Sicherheitsschaltgerät) wird durch einen dynamischen Signalwechsel beim Betätigen des Tasters überwacht. *Anmerkung: Dadurch wird beispielsweise ein Einschalten der Anlage verhindert, das durch einen kurzgeschlossenen Taster (z. B. durch Manipulation) verursacht würde.*	
Teilsystem	**Funktionsblock (FB), SRECS**	**IEC 62061**
	Einheit des Architekturentwurfs des SRECS auf oberster Ebene, wobei ein Ausfall irgendeines Teilsystems zu einem Ausfall der sicherheitsbezogenen Steuerungsfunktion führt. *Anmerkung: Ein vollständiges Teilsystem kann aus einer Anzahl von identifizierbaren und getrennten Teilsystem-Elementen bestehen, die, wenn sie zusammengefügt werden, die zu dem Teilsystem zugeordneten Funktionsblöcke implementieren.*	
Teilsystem-Element	**Teilsystem, SRECS**	**IEC 62061**
	Teil eines Teilsystems, das ein einzelnes Bauteil oder irgendeine Gruppe von Bauteilen umfasst.	
Testung	**Querschluss**	**ISO 13849-1**
	Testpuls mit entsprechender Dunkelzeit zur Fehleraufdeckung.	
Trennende Schutzeinrichtung	**Positionsschalter**	**Feststehende Schutzeinrichtung: EN 294, EN 349, EN 811, EN 953** **Bewegliche Schutzeinrichtung: EN 1088 (ISO 14119), EN 999** **Typ A-Norm: ISO 12100-1**
	Schutzeinrichtung oder der Teil der Maschine, der speziell als körperliche Sperre zum Schutz vor Gefährdung eingesetzt wird. *Anmerkung: Sie kann, je nach Bauart, durch Schutzgitter, Schutztür, Gehäuse, Abdeckung, Verkleidung, Verdeckung, Umzäunung, Schirm usw. realisiert werden.*	
Typ A-Norm **Typ B-Norm** **Typ C-Norm**	**A-Norm** **B-Norm** **C-Norm,** **harmonisierte Norm,** **Vermutungswirkung**	**ISO 12100-1** **ISO 14121** **EN 1070**
	Diese Normen werden in der ISO 12100-1 erwähnt. Damit sind diese Normen in der Maschinenrichtlinie gelistet, und somit harmonisiert.	

U

Begriff	Referenz	relevante Norm
Überwachter Start	Start, Manuelle Rückstellung	ISO 13850, IEC 60204-1, ISO 13849-1
	Das Wiederherstellen der Sicherheitsfunktion erfolgt durch die Überwachung eines dynamischen Signalwechsels, z. B. mit einem Ein-Taster. Für eine Not-Halt-Einrichtung ist dies bei Kategorie 4 nach EN 954-1 zwingend notwendig (Manipulationsschutz). Diese Startart ist nur zulässig nach erfolgter Gefahrenbeurteilung.	

V

Begriff	Referenz	relevante Norm
Vermutungswirkung	MRL, Typ A-B-C Normen	
	Mit Erfüllung der gelisteten, harmonisierten Normen (in der Maschinenrichtlinie) kann vermutet werden, dass die Maschinenrichtlinie erfüllt wurde.	
Verriegelungseinrichtungen	Schutzeinrichtung, Positionsschalter, Zuhaltung	ISO 12100-1 EN 1088 (ISO 14119)
	Ist eine mechanische, elektrische oder andere Verriegelungseinrichtung, deren Zweck es ist, den Betrieb eines Maschinenelementes unter bestimmten Bedingungen zu verhindern (üblicherweise solange eine trennende Schutzeinrichtung nicht geschlossen ist).	
Vorgesehene Architektur	Kategorien, Redundanz	ISO 13849-1
	Die vorgesehenen Architekturen zeigen die logische Darstellung der Systemstruktur für jede Kategorie. Die vorgesehenen Architekturen sind für die zusammengefasste SRP/CS gezeichnet, beginnend an dem Punkt, an dem die sicherheitsbezogenen Signale erzeugt werden und endend am Ausgang der Energieübertragungselemente.	

W

Begriff	Referenz	relevante Norm
Wiederanlaufsperre	Start, Überwachter Start	ISO 13850 IEC 60204-1
	Durch die Wiederanlaufsperre wird die Freigabe der Auswerteeinheit nach einem Abschalten, nach einer Änderung der Betriebsart der Maschine oder nach einem Wechsel der Betätigungsart verhindert. Die Wiederanlaufsperre wird erst durch einen externen Befehl (z. B. EIN-Taster) aufgehoben. *Anmerkung:* *Die ISO 13849-1 spricht von "manueller Rückstellung", einer internen Funktion der SRP/CS zur Wiederherstellung gegebener Sicherheitsfunktionen vor einem Neustart der Maschine.*	
Wiederbereitschaftszeit	Sicherheitsschaltgerät	
	Die notwendige Mindestzeit, um das Gerät neu zu starten, nachdem das Steuerkommando oder die Versorgungsspannung unterbrochen wurde.	

Z

Begriff	Referenz	relevante Norm
Zuhaltung	Positionsschalter	EN 1088 (ISO 14119)
	Ziel einer Zuhaltungseinrichtung ist es, eine trennende Schutzeinrichtung in der geschlossenen Position zu halten. Sie ist außerdem so mit der Steuerung verbunden, dass die Maschine nicht anlaufen kann, wenn die Schutzeinrichtung nicht geschlossen und zugehalten ist und dass die trennende Schutzeinrichtung so lange zugehalten bleibt, bis das Verletzungsrisiko aufgehoben ist. *Anmerkung: Die Ansteuerung der Zuhaltung muss bis Kategorie 3 nach ISO 13849-1 nicht sicher erfolgen, bei Kategorie 4 nach ISO 13849-1 muss diese jedoch immer sicher sein. Die Stellungsüberwachung der Verriegelungseinrichtung (Magnet) muss ab Kategorie 3 nach ISO 13849-1 einzeln erfolgen, nicht in Reihe geschaltet mit der Überwachung des getrennten Betätigers (wegen mangelnder Fehleraufdeckung).*	
Zustimmungsschalter	Auswerteeinheit, Sicherheitsschaltgerät	
	Ein Zustimmungsschalter ist ein manuell betätigter Signalgeber, mit dem die Schutzwirkung von Schutzeinrichtungen bei Betätigung des Signalgebers aufgehoben werden kann. Mit dem Zustimmschalter allein dürfen keine Gefahren bringenden Zustände eingeleitet werden, dafür ist ein "zweiter, bewusster" Startbefehl erforderlich.	
Zwangsgeführte Kontakte	Aktor, Relais	EN 50205, IEC 60947
	Bei zwangsgeführten Kontakten eines Relais/Schütz dürfen Öffner und Schließer über die Lebensdauer niemals gleichzeitig geschlossen sein. Dies gilt auch für den fehlerhaften Zustand der Relais/Schütze. Beispiel: Ist ein Schließer verschweißt, so bleiben alle anderen Öffnerkontakte des betroffenen Relais/Schütz geöffnet, egal ob das Relais/Schütz erregt wird oder nicht.	
Zwangsöffnung ⊖	Positionsschalter, NOT-HALT Befehlsgerät	IEC 60204-1, IEC 60947-5-1
	Ist eine Ausführung einer Kontakttrennung als direktes Ergebnis einer festgelegten Bewegung des Bedienteiles des Schalters über nicht federnde Teile. Für die elektrische Ausrüstung von Maschinen wird die gesicherte Öffnung von Öffnerkontakten in allen Sicherheitskreisen ausdrücklich vorgeschrieben. *Anmerkung: Die Zwangsöffnung ist nach IEC 60947-5-1 durch das Zeichen (Pfeil im Kreis) signalisiert (Personenschutzfunktion).*	
Zweihandschaltung	Synchronüberwachungszeit	EN 574, IEC 60204-1
	Ist eine Einrichtung, die mindestens die gleichzeitige Betätigung (in der Regel < 0,5 s) durch beide Hände erfordert, um den Betrieb einer Maschine ein zu leiten und aufrecht zu erhalten, solange eine Gefährdung besteht. Auf diese Weise wird eine Maßnahme zum Schutz nur der betätigenden Person erreicht. *Anmerkung: Zum Auslösen des gefährlichen Arbeitsganges müssen die beiden Bedienteile (Zweihandtaster) gleichzeitig betätigt werden. Bei Loslassen auch nur eines der beiden Bedienteile während der gefährlichen Bewegung, wird die Freigabe aufgehoben. Die Fortsetzung des gefährlichen Arbeitsganges kann erst wieder eingeleitet werden, wenn beide Bedienteile in ihre Ausgangslage zurückgekehrt sind und erneut betätigt werden.*	
Zweihandbedienpult	Synchronüberwachungszeit, Zweihandschaltung	EN 574
	Ein Gerät zur Realisierung der Zweihandschaltung.	
Zweifehlersicherheit	Kategorie SIL	ISO 13849-1 IEC 62061
	Bedeutet, dass auch nach Auftreten zweier Fehler die vereinbarte sichere Funktion gewährleistet ist.	
Zweikanaligkeit	Redundanz, Kategorien, vorgesehene Architektur	ISO 13849-1

Anhang

4

4.1 Wichtige Typ A, B und C-Normen

Grundnormen (Typ A)		
Gestaltungsgrundsätze, Begriffe	EN ISO 12100-1	Methodik, Terminologie
	EN ISO 12100-2	Technische Leitsätze
	EN 1070	Terminologie 12-sprachig
Gefahrenanalyse, Risikobeurteilung	EN ISO 14121	Leitsätze, Liste der Gefährdungen

Gruppennormen (Typ B1) zu Sicherheitsaspekten		
Brände und Explosionen	EN 1127-1	Explosionsschutz, Methodik
	EN 13463-1	Einsatz von nichtelektrischen Geräten
	EN 13478	Brandschutz
	EN 13821	Mindestzündenergie
Ergonomische Gestaltung	EN 614-1	Gestaltungsgrundsätze
	EN 547-3	Körpermaßdaten
	EN 1005-3	Kraftgrenzen Maschinenbetätigung
	EN ISO 14738	Maschinenarbeitsplätze
Gefahrstoffe	EN 626-1	Reduzierung des Gesundheitsrisikos
	EN 626-2	Überprüfungsverfahren
	EN 1093-1	Luftverunreinigung; Prüfverfahren
Geräusche	EN ISO 3740	Leitlinien Schallleistungsmessung
	EN ISO 4871	Messangaben, Nachprüfung
	EN ISO 11200	Leitlinien, Schalldruckmessung
	EN ISO 11688-1	Lärmarme Konstruktionen
	EN ISO 11689	Emissionsvergleich
Hygiene	EN 1672-2	Nahrungsmittelmaschinen (Typ C-Norm)
Laser	EN 12626	Laserbearbeitungsmaschinen
	EN 60825-1	Lasereinrichtungen
	EN ISO 11553	Laserbearbeitungsmaschinen
Schwingungen	EN 1299	Schwingungsisolierung
Sicherheitsabstände	EN 294	Obere Gliedmaßen
	EN 349	Vermeidung von Quetschungen
	EN 811	Untere Gliedmaßen
	EN 999	Annäherungsgeschwindigkeit
Strahlung	EN 12198-1	Bewertung, Risikominderung
Temperaturen	EN 563	Heiße Oberflächen

Gruppennormen (Typ B2) für Systeme und Schutzeinrichtungen		
Beleuchtung	EN 1837	Maschinenintegrierte Beleuchtung
Elektrische Ausrüstung	EN 60204-1	Allgemeine Anforderungen
Fluidtechnische Ausrüstung	EN 982	Hydraulik
	EN 983	Pneumatik
Schutzeinrichtungen	EN 953	Gestaltung trennender Schutzeinrichtungen
	EN 1088	Verriegelungseinrichtungen
	EN 12874	Flammendurchschlagsicherung
	EN 60825-4	Laserschutzeinrichtungen
	EN 61496-1	Berührungslos wirkende Schutzeinrichtungen
Signale und Stellteile	EN 457	Akustische Gefahrensignale
	EN 842	Optische Gefahrensignale
	EN 894-1	Interaktion mit Anzeigen, Stellteilen
	EN 894-2	Gestaltung von Anzeigen
	EN 894-3	Gestaltung von Stellteilen
	EN 981	Akustische/optische Systeme
	EN 61310-1	Sichtbare, hörbare, tastbare Signale
	EN 61310-2	dto., Kennzeichnung
	EN ISO 13850	Not-Halt Einrichtungen
Steuerungen	EN 574	Zweihandschaltungen
	EN ISO 13849-1	Sicherheitsbezogene Kategorien, Gestaltungsleitsätze
	EN ISO 13849-2	Validierung
	EN 1037	Unerwarteter Anlauf
	EN 1760-1	Schaltmatten, Schaltplatten
	EN 1760-2	Schaltleisten, Schaltstangen
	EN 62061	Sicherheitsbezogene elektrische, elektronische und programmierbare elektronische Steuerungssysteme
Zugänge zu/in Maschinen	EN 547-1	Ganzkörperzugänge
	EN 547-2	Zugangsöffnungen
	EN 547-3	Körpermaßdaten
	EN ISO 14122-1	Zugangswahl zwischen zwei Ebenen
	EN ISO 14122-2	Arbeitsbühnen, Laufstege
	EN ISO 14122-3	Geländer, Treppen, Treppenleitern
	EN ISO 14122-4	Steigleitern

Weitere Typ C Normen sind im Safety Integrated Systemhandbuch zu finden.

4.2 Weitere wichtige Dokumente

- IEC 61326-3-1

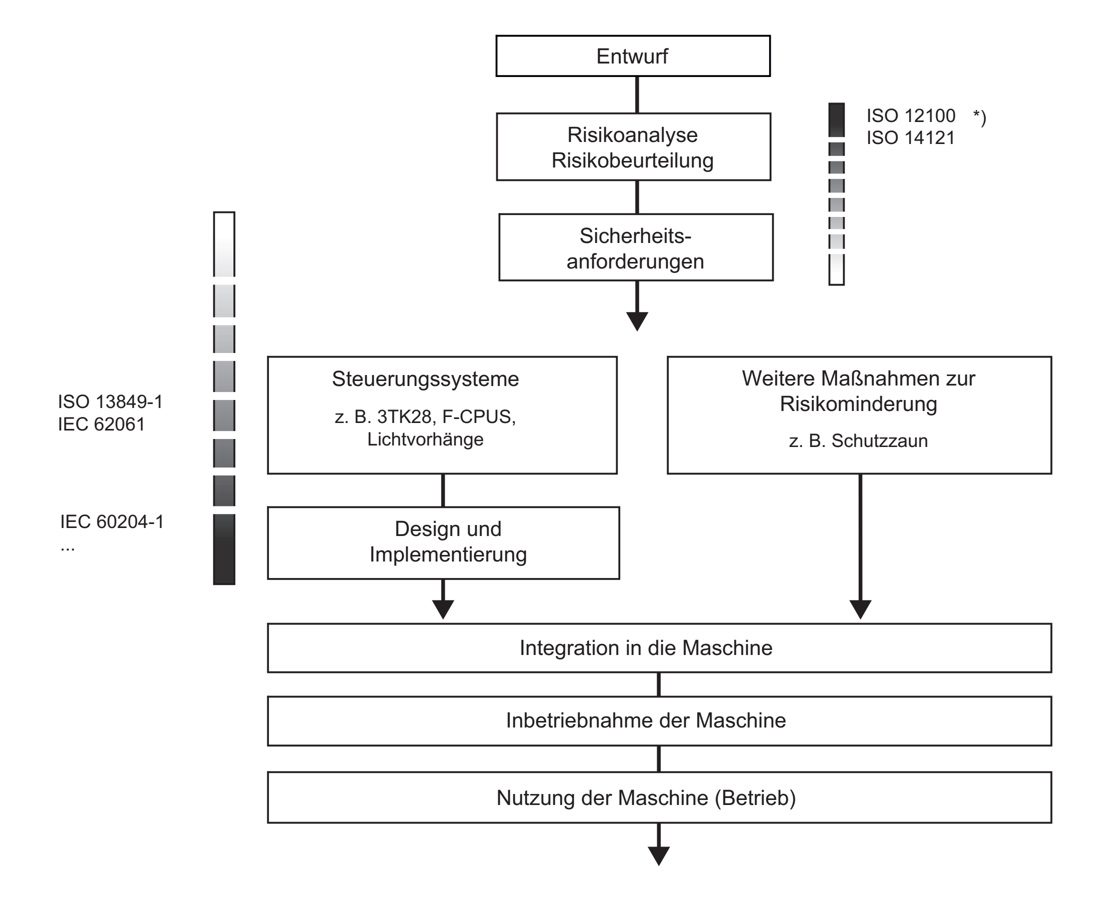
  EMV und Funktionale Sicherheit
- IEC 61508 (VDE 0803)

  Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer, programmierbarer elektronischer Systemen
- ISO Guide 51

  Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen

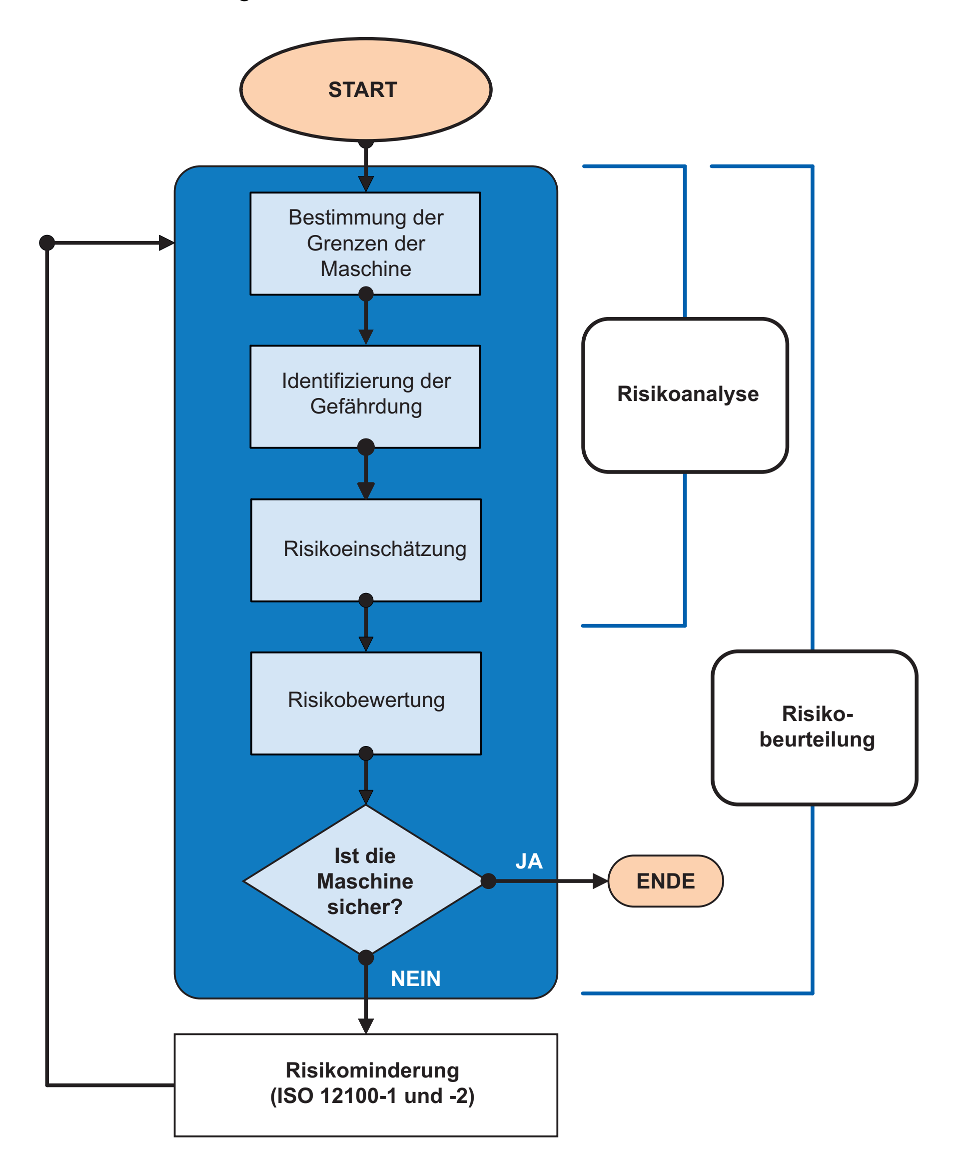
4.3 Risikobeurteilung nach ISO 12100, ISO 14121

Lebenszyklus einer Maschine



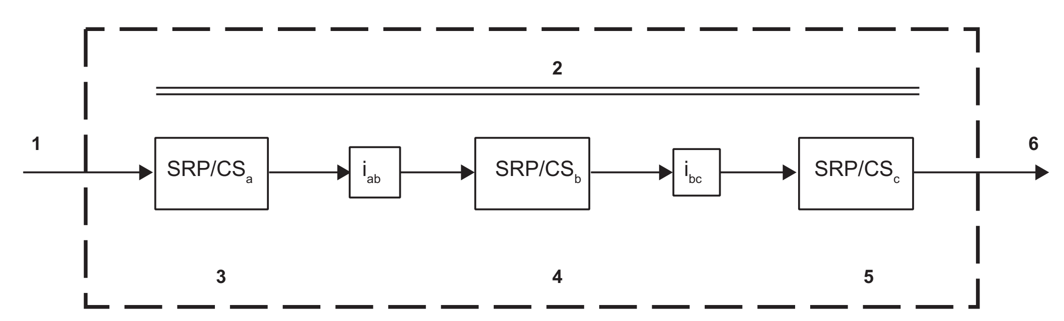
Prozess der Risikoreduzierung

Risikoreduzierung nach der ISO 14121



4.4 Performance Level Bestimmung

Sicherheitsfunktion nach ISO 13849-1



1 Mittel zur Initiierung, z. B. manuelle Eingabe
2 Typische Sicherheitsfunktion (Eingang, Logik, Ausgang)
3 Eingang
4 Logik
5 Ausgang
6 Maschinenaktor, Abschalteinrichtung, Bremse(n)

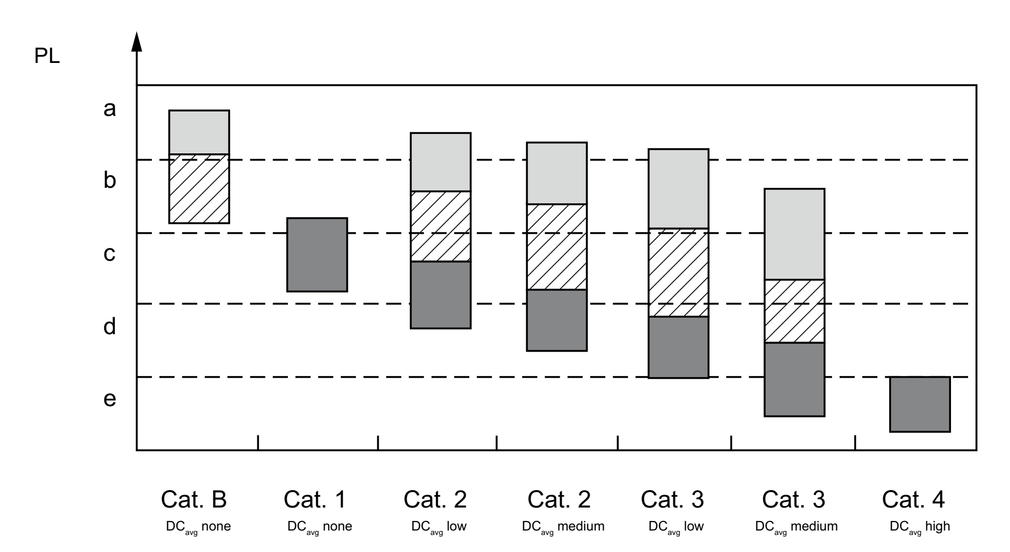
Performance Level und SIL Zuordnung nach ISO 13849-1

Performance Level PL	Durchschnittliche Wahrscheinlichkeit eines Gefahr bringenden Ausfalls je Stunde [1/h]	SIL (EN 61508-1) zur Information
a	$\geq 10^{-5} \ldots < 10^{-4}$	keine speziellen Sicherheitsanforderungen
b	$\geq 3 \cdot 10^{-6} \ldots < 10^{-5}$	1
c	$\geq 10^{-6} \ldots < 3 \cdot 10^{-6}$	1
d	$\geq 10^{-7} \ldots < 10^{-6}$	2
e	$\geq 10^{-8} \ldots < 10^{-7}$	3

Anmerkung 1:
Die Höhe der Gefährdungssituation wird in dieser Norm in fünf Stufen von a bis e geteilt, wobei die Risikominderung als Beitrag durch die SRP/CS bei a niedrig und bei e hoch ist.

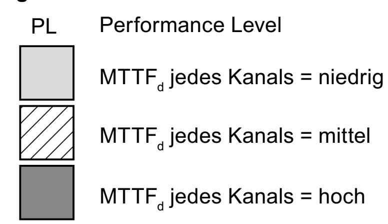
Anmerkung 2:
Es sollte beachtet werden, dass die Performance Level b und c zusammen nur eine Größenordnung der Einheit der durchschnittlichen Wahrscheinlichkeit eines Gefahr bringenden Ausfalls je Stunde (oder eine Stufe auf der SIL-Skala) abdecken.

Zuordnung Performance Level ↔ Kategorie (in Funktion von DC und MTTFd) nach ISO 13849-1



Legende

PL Performance Level



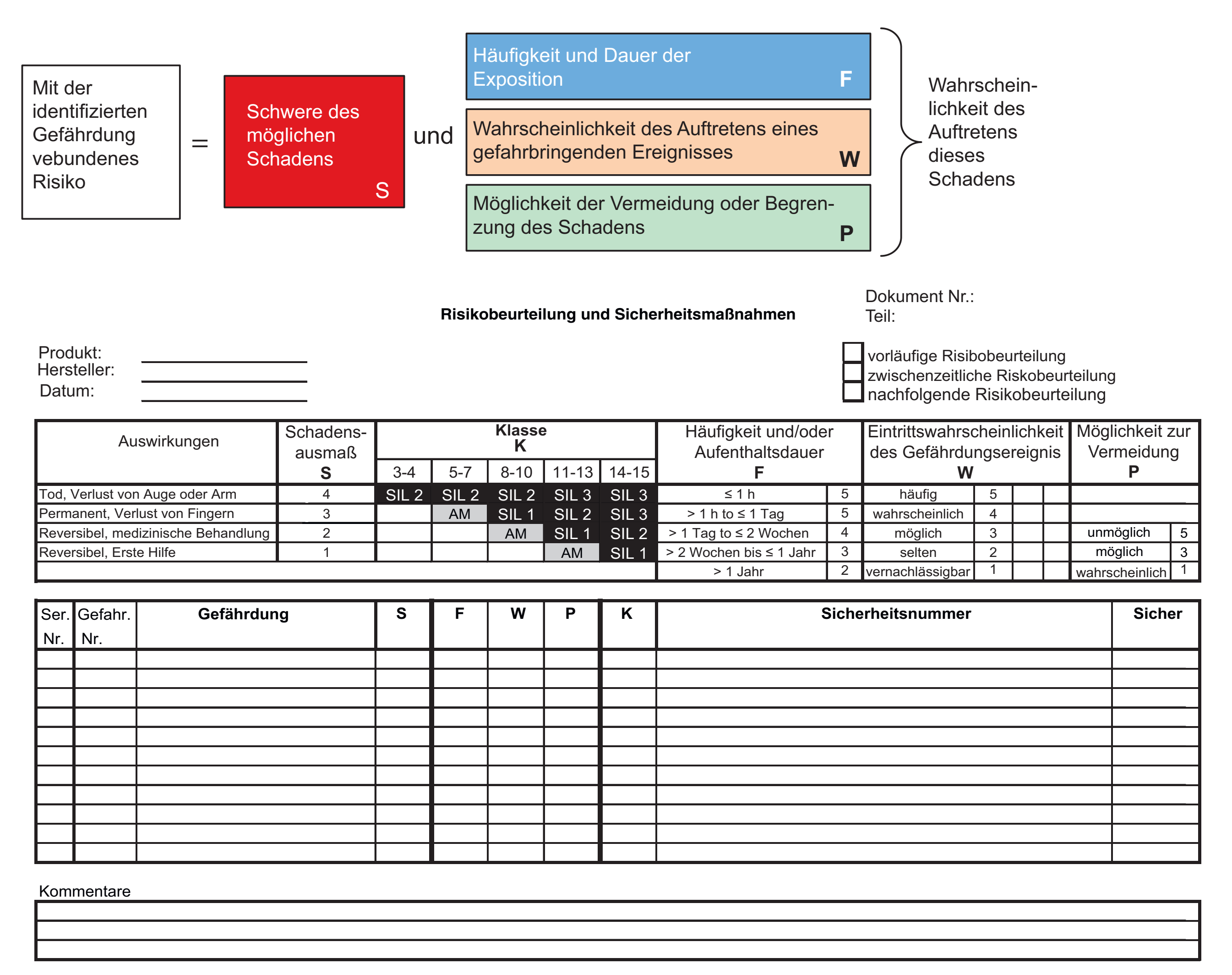
$MTTF_d$ jedes Kanals = niedrig

$MTTF_d$ jedes Kanals = mittel

$MTTF_d$ jedes Kanals = hoch

4.5 SIL Zuordnung

SIL Einschätzung nach IEC 62061



Risikobeurteilung und Sicherheitsmaßnahmen

Dokument Nr.:
Teil:

Produkt: ______
Hersteller: ______
Datum: ______

☐ vorläufige Risibobeurteilung
☐ zwischenzeitliche Riskobeurteilung
☐ nachfolgende Risikobeurteilung

Auswirkungen	Schadens-ausmaß **S**	**Klasse K** 3-4	5-7	8-10	11-13	14-15	Häufigkeit und/oder Aufenthaltsdauer **F**		Eintrittswahrscheinlichkeit des Gefährdungsereignis **W**				Möglichkeit zur Vermeidung **P**	
Tod, Verlust von Auge oder Arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	≤ 1 h	5	häufig	5				
Permanent, Verlust von Fingern	3		AM	SIL 1	SIL 2	SIL 3	> 1 h to ≤ 1 Tag	5	wahrscheinlich	4				
Reversibel, medizinische Behandlung	2			AM	SIL 1	SIL 2	> 1 Tag to ≤ 2 Wochen	4	möglich	3			unmöglich	5
Reversibel, Erste Hilfe	1				AM	SIL 1	> 2 Wochen bis ≤ 1 Jahr	3	selten	2			möglich	3
							> 1 Jahr	2	vernachlässigbar	1			wahrscheinlich	1

Ser. Nr.	Gefahr. Nr.	**Gefährdung**	**S**	**F**	**W**	**P**	**K**	**Sicherheitsnummer**	**Sicher**

Kommentare

SIL und PFH$_D$

Sicherheits-Integritätslevel (SIL)	Wahrscheinlichkeit eines Gefahr bringenden Ausfalls pro Stunde
1	$10^{-6} \leq PFH_D < 10^{-5}$
2	$10^{-7} \leq PFH_D < 10^{-6}$
3	$10^{-8} \leq PFH_D < 10^{-7}$

Ausfallwahrscheinlichkeit elektromechanischer Komponenten

Ausfallrate
$\lambda = 0{,}1 \cdot C/B10$
$\lambda = 0{,}1 \cdot 10/10^6 = 10^{-6}$ C: Cycle, Betätigungszyklus pro Stunde B10: Anzahl Betätigungszyklen nach denen 10 % der Geräte ausgefallen sind (IEC 61810-2)
Ausfallwahrscheinlichkeit (gefährlich, in einer Stunde)
$PFH_D = \lambda_D \cdot 1h$
$\lambda = \lambda_s + \lambda_d$ λ_s sichere Hardwareausfälle λ_d Gefahr bringende Ausfälle

Architektur A: Nullfehlertoleranz, ohne Diagnose-Funktion (vgl. Kategorie 1) Nullfehlertoleranz: Ein Fehler führt zum Verlust der Sicherheitsfunktion Diagnose: Ohne Fehleraufdeckung
$\lambda_D = \lambda_{D1} + \ldots + \lambda_{Dn}$

Architektur B: Einfehlertoleranz, ohne Diagnose-Funktion Einfehlertoleranz: Ein Fehler führt nicht zum Verlust der Sicherheitsfunktion Diagnose: Ohne Fehleraufdeckung
$\lambda_D = (1 - \beta)^2 \cdot \lambda_{De1} \cdot \lambda_{De2} \cdot T1 + \beta \cdot (\lambda_{De1} + \lambda_{De2})/2$
β: Faktor der Fehler gemeinsamer Ursache T_1: Lebenserwartungszeit

Architektur C: Nullfehlertoleranz, mit Diagnose-Funktion (vgl. Kategorie 2) Nullfehlertoleranz: Ein Fehler führt zum Verlust der Sicherheitsfunktion Diagnose: Mit Fehleraufdeckung
$\lambda_D = \lambda_{De1} \cdot (1 - DC_1) + \ldots + \lambda_{Den} \cdot (1 - DC_n)$
DC: Diagnosedeckungsgrad

Architektur D: Einfehlertoleranz, mit Diagnose-Funktion (vgl. Kategorie 3/4) Einfehlertoleranz: Ein Fehler führt nicht zum Verlust der Sicherheitsfunktion Diagnose: Mit Fehleraufdeckung
$\lambda_D = (1 - \beta)^2 \cdot \{[\lambda_{De1} \cdot \lambda_{De2} \cdot (DC_1 + DC_2) \cdot T_2/2] + [\lambda_{De1} \cdot \lambda_{De2} \cdot (2 - DC_1 - DC_2) \cdot T_1/2]\} + \beta \cdot (\lambda_{De1} + \lambda_{De2})/2$
T_2: Diagnose Testintervall

4.6 Antriebssteuerungen mit integrierten Sicherheitsfunktionen

Definition der Sicherheitsfunktionen in IEC 61800-5-2, Adjustable speed electrical power drive systems, Safety Requirements, Functional.

Abk.	Bezeichnung	DE	Funktion
STO	Safe torque off	Sicher abgeschaltetes Moment	Motor erhält keine Energie, die eine Drehbewegung erzeugt (Stopp-Kat 0 nach IEC 60204)
SS1	Safe Stop 1	Sicherer Stopp 1	Motor verzögert; Überwachung Bremsrampe und STO nach Stillstand oder STO nach Ablauf einer Verzögerungszeit (Stopp-Kat 1 nach IEC 60204)
SS2	Safe Stop 2	Sicherer Stopp 2	Motor verzögert; Überwachung Bremsrampe und SOS nach Stillstand oder SOS nach Ablauf einer Verzögerungszeit (Stopp-Kat 2 nach IEC 60204)
SOS	Safe Operating Stop	Sicherer Betriebshalt	Motor steht still und widersteht externen Kräften
SLS	Safely-Limited Speed	Sicher begrenzte Geschwindigkeit	Das Überschreiten eines Geschwindigkeits-Grenzwerts wird verhindert
SLT	Safely-Limited Torque	Sicher begrenztes Moment	Das Überschreiten eines Drehmoment/Kraft-Grenzwerts wird verhindert
SLP	Safely-Limited Position	Sicher begrenzte Position	Das Überschreiten eines Positions-Grenzwerts wird verhindert
SLI	Safely-Limited Increment	Sicher begrenztes Schrittmaß	Der Motor wird um ein spezifiziertes Schrittmaß verfahren und stoppt anschließend
SDI	Safe Direction	Sichere Bewegungsrichtung	Der Motor kann nur in die spezifizierte Richtung verfahren werden
SMT	Safely Motor Temperature	Sichere begrenzte Motortemperatur	Das Überschreiten eines Motortemperatur-Grenzwerts wird verhindert
SBC	Safe Brake Control	Sichere Bremsenansteuerung	Sichere Ansteuerung einer externen Bremse
SCA	Safe Cam	Sicherer Nocken	Die Position des Motors in einem spezifiziertem Bereich wird durch ein sicheres Ausgangssignal angezeigt (Sicherer Nocken)
SSM	Safe speed monitor	Sichere Rückmeldung der begrenzten Geschwindigkeit	Die Drehzahl des Motors unterhalb eines spezifizierten Wertes wird durch ein sicheres Ausgangssignal angezeigt

1. Weitere Sicherheitsfunktionen sind zulässig.
2. Keine Unterscheidung zwischen Sicherheitsfunktionen für Maschinen und Prozess.
3. Reaktion bei Verletzung eines Grenzwerts:

   Muss individuell festgelegt werden, da optimale Reaktion abhängig von Gerätearchitektur und Applikation.
4. Reaktion bei Fehler der Sicherheitsfunktion:

   Muss individuell festgelegt werden, da optimale Reaktion abhängig von Gerätearchitektur und Applikation.

4.7 Bewertung von Sicherheitsfunktionen mit dem Safety Evaluation Tool

Beschreibung der Funktionalität

Bei der Bewertung von Sicherheitsfunktionen an Maschinen und Anlagen bietet Ihnen die schnelle und einfache Handhabung des SIEMENS Safety Evaluation Tool wertvolle Unterstützung.

Das TÜV-geprüfte Online-Tool führt den Anwender schrittweise von der Festlegung der Struktur des Sicherheitssystems, über die Auswahl der Komponenten zur Ermittlung der erreichten Sicherheitsintegrität gemäß ISO 13849-1 und IEC 62061. Die Vorgehensweise ist für beide Normen hinsichtlich der Handhabung gleich. Im Vordergrund steht eine schnelle, einfach nachvollziehbare Bewertung einer ausgewählten Sicherheitsfunktion.

Alle Siemens Produktdaten sind direkt online verfügbar, aber auch die Verwendung von anderen Herstellerkomponenten ist problemlos möglich. Hierbei unterstützen Sie auch die integrierten umfangreichen Beispiel-Bibliotheken. Als Ergebnis erhält der Benutzer einen normenkonformen Report, der als Sicherheitsnachweis in die Dokumentation integriert werden kann.

Durch den Online-Zugriff des Safety Evaluation Tool ist sichergestellt, dass die Berechnungen immer mit der aktuellen Normenlage durchgeführt werden und das stehts auf die aktuellen technischen Daten aller sicherheitsrelevanten Komponenten von Siemens zugegriffen wird.

Die Anwendung der Normen und der Einsatz zertifizierter Produkte minimieren Aufwand und Risiko. Siemens Safety Integrated Produkte sind nach den relevanten Herstellernormen zertifiziert und mit Herstellerangaben im Tool bequem aufrufbar.

Voraussetzungen

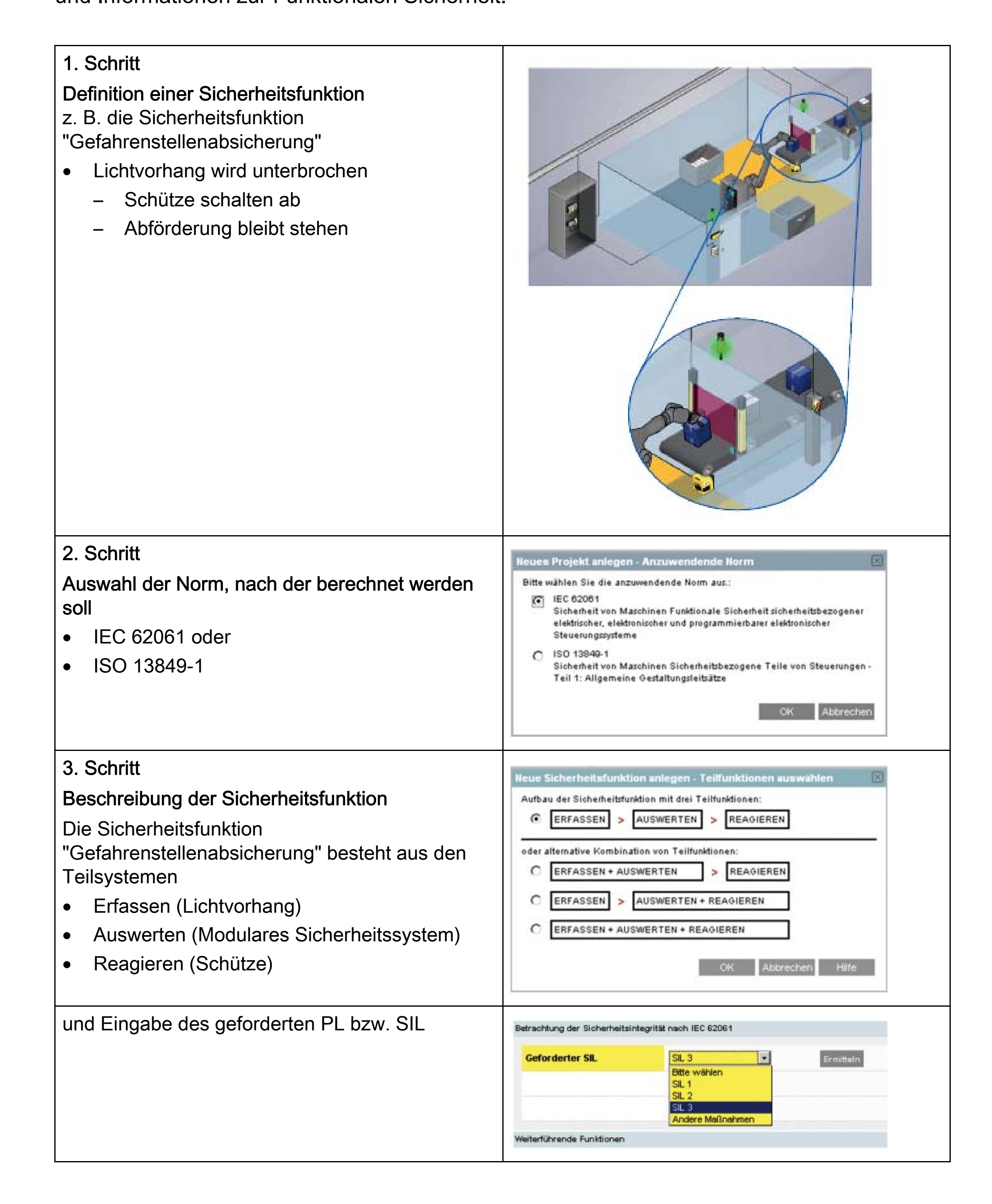
Voraussetzung für den Einsatz des Safety Evaluation Tool ist eine zuvor durchgeführte Gefahrenbeurteilung (Risikoanalyse), in der die resultierenden Sicherheitsfunktionen definiert werden. Hier sind grundsätzlich die logischen Funktionen mit den bereits angedachten Hardware-Teilfunktionen (z. B. Erfassen, Auswerten und Reagieren) auszuwählen.

Ebenso sind die Verantwortlichen (Projektverantwortlicher und Projektprüfer) für die anschließenden Abnahmeprüfungen zu benennen.

Aufruf des Safety Evaluation Tool

www.siemens.com/safety-evaluation-tool

Hier können Sie sich für das Tool anmelden und das Tool starten. Außerdem finden Sie dort Information rund um das Tool, beispielsweise eine Broschüre, ein Leitfaden zur Bedienung und Informationen zur Funktionalen Sicherheit.



1. Schritt **Definition einer Sicherheitsfunktion** z. B. die Sicherheitsfunktion "Gefahrenstellenabsicherung" • Lichtvorhang wird unterbrochen – Schütze schalten ab – Abförderung bleibt stehen	
2. Schritt **Auswahl der Norm, nach der berechnet werden soll** • IEC 62061 oder • ISO 13849-1	
3. Schritt **Beschreibung der Sicherheitsfunktion** Die Sicherheitsfunktion "Gefahrenstellenabsicherung" besteht aus den Teilsystemen • Erfassen (Lichtvorhang) • Auswerten (Modulares Sicherheitssystem) • Reagieren (Schütze)	
und Eingabe des geforderten PL bzw. SIL	

4. Schritt

Anlegen der Teilsysteme bzw. der SRP/CS, Erfassen, Auswerten und Reagieren

Dateneingabe:
Produktauswahl aus Datenbank

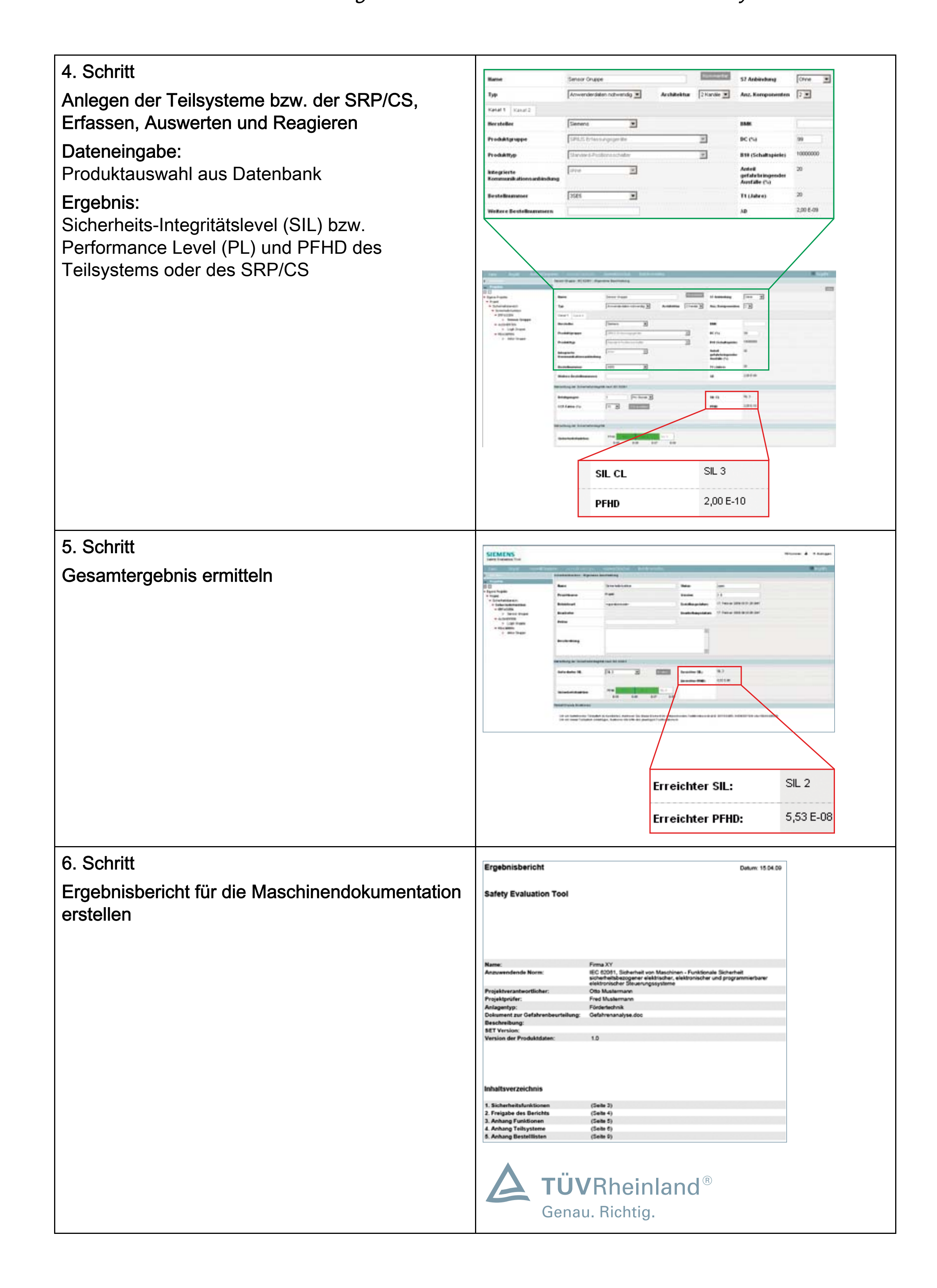
Ergebnis:
Sicherheits-Integritätslevel (SIL) bzw. Performance Level (PL) und PFHD des Teilsystems oder des SRP/CS

5. Schritt

Gesamtergebnis ermitteln

6. Schritt

Ergebnisbericht für die Maschinendokumentation erstellen



Safety Evaluation Tool – Vorteile auf einen Blick

- Sicherheit beim Umgang mit den Normen: Automatische Berechnung nach aktueller Normenlage
- Schnelles Ergebnis: normenkonformer Bericht
- TÜV-geprüftes Tool
- Zeitersparnis bei der Bewertung von Sicherheitsfunktionen
- Schneller Zugriff auf aktuelle Produktdaten
- Komfortable Archivierung: Projekte können gespeichert und bei Bedarf wieder aufgerufen werden
- Schnelle und einfache Handhabung: umfangreiche, vordefinierte Beispielbibliotheken
- Kostenfreie Nutzung des Online-Tools
- Weltweiter Service und Support

4.8 Wörterbuch Englisch - Deutsch

Englisch	Deutsch
Access to a hazard zone (to a danger zone)	Zugang zu einem Gefährdungsbereich
Access means	Zugänge
Access code	Zugangscode
Accessibility	Zugänglichkeit
Active opto-electronic protective device	Aktive optoelektronische Schutzeinrichtung
Actuator/manual control	Stellteil
Actuator (Machine -)	Antriebselement
Adequate risk reduction	Entsprechende Risikominderung
Adjustable guard	Einstellbare trennende Schutzeinrichtung
Angular part	Spitzes Teil
Application point	Befestigungspunkt
Assembly of machines	Maschinenanlage
Barrier	Sperre
Burn	Verbrennung
Centre of gravity	Masseschwerpunkt
Cleaning	Reinigung
Colour	Farbe
Commissioning	Inbetriebnahme
Common cause failures	Ausfälle aufgrund gemeinsamer Ursache
Common mode failures	Gleichartige Ausfälle
Comparative emission data	Vergleichende Emissionsdaten
Complementary protective measures	Ergänzende Schutzmaßnahmen
Construction	Bau
Containment (of materials, etc.)	Kapselung/Fernhaltung (von Stoffen, usw.)
Containment (of stored energy)	Rückhaltung (von gespeicherter Energie)
Control	Steuerung
Control device	Steuereinrichtung, Steuerungseinrichtung
Control guard (see also: interlocking guard with a start function)	Steuernde trennende Schutzeinrichtung (siehe auch: trennende Schutzeinrichtung mit Startfunktion)
Control mode	Steuerungsart
Control system	Steuersystem/Steuerung
Critical component	Kritisches Bauteil
Crushing hazard	Gefährdung durch Quetschen
Cutting element	Schneidelement
Cutting/severing hazard	Gefährdung durch Schneiden
Damage to health	Gesundheitsschädigung
Danger	Gefahr
Danger zone (see also: hazard zone)	Gefährdungsbereich
De-commissioning	Außerbetriebnahme

Englisch		Deutsch
Defeating (of a protective device)		Umgehen (einer Schutzeinrichtung)
Defeating (of a warning device)		Umgehen (einer Warneinrichtung)
Depressurizing		Druckentlastung
Design (of a machine)		Konstruktion (einer Maschine)
Design error		Konstruktionsfehler
Designer		Konstrukteur/Entwickler
Diagnostic system		Diagnosesystem
Direct contact		Direktes Berühren
Display		Anzeige
Disposal (of a machine)		Entsorgung (einer Maschine)
Disturbance(s)		Störung(en)
Door		Tür
Drawing-in/trapping hazard		Gefährdung durch Einziehen/Fangen
Dust		Staub
Edge (sharp -)		Kante (scharfe -)
Electric shock		Elektrischer Schlag
Electrical equipment		Elektrische Ausrüstung
Electrical hazard		Elektrische Gefährdung
Electrical hazard (Preventing -)		Elektrische Gefährdung (Verhütung von -)
Electrical overloading		Elektrische Überlastung
Electromagnetic compatibility		Elektromagnetische Verträglichkeit
Emergency operation		Handlung im Notfall
Emergency situation		Notfall
Emergency stop (function)		Stillsetzen im Notfall (Funktion zum -)
Emergency stop control		Stellteil zum Stillsetzen im Notfall
Emergency stop device		Einrichtung zum Stillsetzen im Notfall
Emissions		Emissionen
Emission value		Emissionswert
Enabling device		Zustimmungseinrichtung
Entanglement hazard		Gefährdung durch Erfassen
Environment		Umgebung
Environmental conditions		Umgebungseinflüsse
Ergonomic principle		Ergonomischer Grundsatz
Error (Human)		Fehlverhalten (menschliches -)
Escape and rescue (of a person)		Befreiung und Rettung (einer Person)
Explosive atmosphere		Explosionsfähige Atmosphäre
Exposure to hazard		Gefährdungsexposition/Aussetzung einer Gefährdung
Exposure to hazards (Limiting -)		Gefährdungsexposition (Begrenzung der -)
Exposure value		Immissionswert
Failure		Ausfall
Failure to danger		Gefahrbringender Ausfall

Englisch	Deutsch
Falling hazard	Sturzgefährdung
Fault	Fehler
Fault finding	Fehlersuche
Fixed guard	Feststehende trennende Schutzeinrichtung
Foundation	Fundament
Friction/abrasion hazard	Gefährdung durch Reibung/Abrieb
Guard	Trennende Schutzeinrichtung
Guard locking device	Zuhalteeinrichtung
Handling	Handhabung
Harm	Schaden
Hazard	Gefährdung
Hazard combination	Gefährdungskombination
Hazard identification	Identifizierung der Gefährdungen
Hazardous substances	Gefahrstoffe
Hazards generated by materials and substances	Gefährdung durch Materialien und Substanzen
Hazards generated by neglecting ergonomic principles	Gefährdung durch Vernachlässigung ergonomischer Grundsätze
Hazards generated by noise	Gefährdung durch Lärm
Hazards generated by radiation	Gefährdung durch Strahlung
Hazards generated by vibration	Gefährdung durch Vibration
Hazard zone (see also: danger zone)	Gefährdungsbereich
Hazardous malfunctioning	Gefährdung durch Fehlfunktion(en)
Hazardous situation	Gefährdungssituation/gefährdende Situation
Heat	Hitze
Heat source	Wärmequelle
High pressure fluid ejection hazard	Gefährdung durch Herausspritzen von Flüssigkeiten unter hohem Druck
Hold-to-run control device	Befehlseinrichtung mit selbsttätiger Rückstellung (Tippschalter)
Human behaviour	Menschliches Verhalten
Hydraulic equipment	Hydraulische Ausrüstung
Impact	Stoß
Impact hazard	Gefährdung durch Stoß
Impeding device	Abweisende Schutzeinrichtung (Barriere)
Index (of the instruction handbook)	Stichwortverzeichnis (in der Betriebsanleitung)
Indirect contact	Indirekte Berührung
Information for use	Benutzerinformation
Inherent design measure	Maßnahme zur eigensicheren Konstruktion
Inspection	Inspektion
Inspection (Frequency of -)	Inspektion (Häufigkeit der -)
Installation (of the machine)	Aufbau/Einbau (der Maschine)
Instruction handbook	Betriebsanleitung
Instructions	Anweisungen

Englisch		Deutsch
Insulation failure		Isolationsfehler
Intended use of a machine		Bestimmungsgemäße Verwendung einer Maschine
Interlocking device (interlock)		Verriegelungseinrichtung (Verriegelung)
Interlocking guard		Verriegelte trennende Schutzeinrichtung
Interlocking guard with guard locking		Verriegelte trennende Schutzeinrichtung mit Zuhaltung
Interlocking guard with a start function (see also: control guard)		Trennende Schutzeinrichtung mit Startfunktion (siehe auch: steuernde trennende Schutzeinrichtung)
Isolation and energy dissipation		Energietrennung und -abbau
Language		Sprache
Language (of the instruction handbook)		Sprache (der Betriebsanleitung)
Life limit of a machine		Lebensdauer einer Maschine
Lifting equipment		Hebevorrichtung
Lifting gear		Hebezeug
Lighting		Beleuchtung
Limit		Grenze
Limited movement control device		Schrittschaltung
Limiting device		Begrenzungseinrichtung
Live part (of electrical equipment)		Spannungsführendes Teil (der elektrischen Ausrüstung)
Load		Last
Loading (feeding)/unloading (removal) operations		Be-/Entladearbeit (Beschickungs- und Entnahmearbeiten)
Lubrication		Schmierung
Machine/machinery		Maschine
Machine-power supply interface		Schnittstelle "Maschine-Energieversorgung"
Maintainability (of a machine)		Instandhaltbarkeit (einer Maschine)
Maintenance		Instandhaltung
Maintenance point		Wartungsstelle
Maintenance staff		Instandhaltungspersonal
Malfunction (malfunctioning)		Fehlfunktion
Manual control (function)		Handsteuerung
Manual control (Actuator)		Stellteil
Marking		Zeichen
Markings		Kennzeichnungen
Material		Werkstoff/Material
Maximum speed of rotating parts		Maximale Drehzahl rotierender Teile
Measurement methods		Messmethoden
Mechanical hazard		Mechanische Gefährdung
Mechanical restraint device		Durch Formschluß wirkende Schutzeinrichtung
Mirror Contact		Spiegelkontakt

Englisch	Deutsch
Mode selector	Betriebsartenschalter
Moisture	Feuchtigkeit
Movable elements/parts	Bewegliche Elemente/Teile
Movable guard	Bewegliche trennende Schutzeinrichtung
Noise	Geräusch
Normal operation	Normaler Betrieb
Operating modes	Betriebsarten
Operation	Betreiben
Operative part	Betriebsteil
Operator	Bedienperson
Operator-machine interface	Schnittstelle "Bedienperson-Maschine" oder "Mensch-Maschine"
Oriented failure mode component	Bauteil mit definiertem Ausfallverhalten
Overloading (Electrical -)	Überlast (Elektrische -)
Overloading (Mechanical -)	Überlastung (Mechanische -)
Overspeed	Überdrehzahl
Packaging (action)	Verpacken (Tätigkeit)
Packaging	Verpackung
Pictogram	Piktogramm
Platform	Bühne/Arbeitsbühne
Pneumatic equipment	Pneumatische Ausrüstung
Portable control unit (teach pendant)	Tragbare Steuereinheit/Tragbares Steuergerät (Schwenkarmschalttafel)
Positive mechanical action	Mechanisch zwangsläufige Wirkung
Positive mode (Connected in the -)	Zwangsläufig (verbunden)
Positively Driven Contact	Zwangsgeführter Kontakt
Power control element	Leistungssteuerelement
Power supply	Energieversorgung/Energiequelle
Power transmission element	Energieübertragungselement
Pressure sensitive mat	Schaltmatte
Prevention of access	Verhinderung des Zugangs
Process changeover	Umrüsten
Programmable electronic control system	Programmierbares elektronisches Steuersystem
Prohibited usage/application	Verbotene Anwendung
Protective device	Nicht trennende Schutzeinrichtung
Protective measure	Schutzmaßnahme
Protruding part	Vorstehendes Teil
Radiation	Strahlung
Range of applications	Anwendungsbereich
Reasonably foreseeable misuse	Vernünftigerweise vorhersehbarer Missbrauch
Rectification (Fault -)	(Fehler-) Behebung
Reduced speed	Verminderte Geschwindigkeit

Englisch		Deutsch
Redundancy		Redundanz
Relevant hazard		Relevante Gefährdung
Reliability (of a machine)		Zuverlässigkeit (einer Maschine)
Rescue and escape (of a person)		Rettung und Befreiung (einer Person)
Residual risk		Restrisiko
Restart/restarting		Wiederanlauf
Restriction of access		Zugangsbeschränkung
Risk		Risiko
Risk analysis		Risikoanalyse
Risk assessment		Risikobeurteilung
Risk comparison		Risikovergleich
Risk estimation		Risikoeinschätzung
Risk evaluation		Risikobewertung
Risk reduction		Risikominderung
Safeguard		Schutzeinrichtung
Safeguarding		Technische Schutzmaßnahmen
Safety function (safety critical function)		Sicherheitsfunktion (direkt wirkende -)
Scald		Verbrühung
Sensitive protective equipment		Berührungslos wirkende Schutzeinrichtung
Sensor		Sensor/Messfühler
Setting		Einrichten/Einstellen
Setting (Control mode for -)		Einstellen (Steuerungsart zum -)
Setting point		Einricht-/Einstellungspunkt
Severing hazard		Gefährdung durch Abschneiden
Shearing hazard		Gefährdung durch Scheren
Signal		Signal
Significant hazard		Signifikante Gefährdung
Siren		Sirene
Slipping hazard		Gefährdung durch Ausrutschen
Software		Software
Software (Access to the -)		Software (Zugriff auf/zur -)
Space limit		Räumliche Grenze
Speed		Geschwindigkeit
Stabbing/puncture hazard		Gefährdung durch Durchstich/Einstich
Stability		Standfestigkeit/Standsicherheit
Stairs		Treppen
Static electricity		Statische Elektrizität
Stopping		Stillsetzen
Storage (of a machine)		Lagerung (einer Maschine)
Stress (human -)		Stress
Stress (Environmental -)		Umweltbeanspruchung
Stress (Mechanical -)		Mechanische Beanspruchung

Englisch		Deutsch
Symbol		Symbol
Symbol (in the instruction handbook)		Symbol (in der Betriebsanleitung)
Teach pendant (portable control unit)		Schwenkarmschalttafel (Tragbare Steuereinheit/Tragbares Steuergerät)
Teaching (programming)		Unterweisung/Programmierung/Eingeben
Thermal hazard		Thermische Gefährdung
Training		Ausbildung
Transport		Transport
Trip/tripping device		Schutzeinrichtung mit Annäherungsreaktion
Trip/tripping hazard		Gefährdung durch Stolpern
Tripping (function)		Annäherungsreaktion
Two-hand control device		Zweihandschaltung
Unexpected/unintended start-up		Unerwarteter/unbeabsichtigter Anlauf
Unloading (removal)/loading (feeding) operations		Ent-/Beladearbeit (Entnahme- und Beschickungsarbeiten)
Usability (of a machine)		Benutzerfreundlichkeit (einer Maschine)
Use (of a machine)		Verwendung (einer Maschine)
User		Benutzer
Valve		Ventil
Vapour (gas)		Dampf (Gas)
Vibration		Vibration
Walking area		Gehbereich
Walkways		Fußgängerwege/Laufstege
Warning		Warnhinweis
Warning device		Warneinrichtung
Work environment		Arbeitsumgebung
Working part		Arbeitsteil
Written warning		Schriftlicher Warnhinweis

4.9 Bewertung/Rückmeldung

Technical Assistance

I IA CE MK&ST 1

D-90327 Fürth

Fax: +49 (911) 895-5907

Absender

Name:

Dienststelle:

Ort:

Telefon:

Internetadresse:

Sollten Sie beim Lesen dieser Unterlage auf Druckfehler gestoßen sein, bitten wir Sie, uns diese mit diesem Vordruck mitzuteilen. Ebenso dankbar sind wir für Anregungen und Verbesserungsvorschläge.

Bewertung der Schrift „Einführung und Begriffe zur funktionalen Sicherheit von Maschinen und Anlagen“

Finde ich sehr gut ❑ Finde ich gut ❑ Finde ich nicht so gut ❑

Weil:

Zeitersparnis durch Verwendung des Dokumentes:

Keine Ersparnis ❑ ca. 5 % ❑ ca. 10 % ❑ andere...........%

Anregungen:

Siemens AG
Industry Sector
Safety Integrated
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

Änderungen vorbehalten
E86060-T1813-A101-A3
X.8215.01.04 / Dispo 27610
KG 0910 2. ROT 92 DE
Printed in Germany

www.siemens.de/safety-integrated